Jurnal Fokus Elektroda : Energi Listrik, Telekomunikasi, Komputer, Elektronika dan Kendali)
Volume 07 No 04, Tahun 2022: Hal. 212-218
e-ISSN: 2502-5562. Open Access at: https://elektroda.uho.ac.id/
Penerbit : Jurusan Teknik Elektro Universitas Halu Oleo Kendari Sulawesi Tenggara,

Application of VPN based on L2TP untuk Mengakses e-Rapor di SMKN 5 Semarang

Eva Elkana[1] dan Djoko Adi Widodo[2]

[1] Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Semarang, [2] Pendidikan Teknik Elektro, Universitas Negeri Semarang

Coprespondent Author: evaelkana@gmail.com

Abstract* — *No password security on the IP caused the e-Report of SMKN 5 Semarang to be hacked. Previously, the SMKN 5 Semarang network used an IP public, not yet using VPN technology. This research applies VPN technology based on L2TP in the network of SMKN 5 Semarang. The network design method uses PPDIOO. Before accessing e-Report, the teachers must be connected to the L2TP VPN, then type 192.168.11.3:3799 on the browser. L2TP was successfully implemented based on the ping test results and e-Report access. Not only got secure because the data is encrypted, but teachers can also access it anywhere.

Keyword* — *e-Rapor, L2TP, PPDIOO, VPN

Abstrak — Tidak adanya password keamanan pada IP menyebabkan e-Rapor SMKN 5 Semarang diretas. Sebelumnya, jaringan SMKN 5 Semarang menggunakan IP Publik, belum menggunakan teknologi VPN. Penelitian ini mengaplikasikan teknologi VPN berbasis L2TP di jaringan SMKN 5 Semarang. Desain jaringan dirancang menggunakan metode PPDIOO. Sebelum mengakses e-Rapor, guru harus terhubung dengan VPN L2TP, kemudian mengetik 192.168.11.3:3799 pada browser. L2TP berhasil diterapkan berdasarkan hasil pengujian tes *ping* dan berhasil mengakses e-Rapor. Tidak hanya mendapatkan keamanan, guru juga dapat mengakses e-Rapor ini di mana saja.

Kata kunci — e-Rapor, L2TP, PPDIOO, VPN

I. PENDAHULUAN

Seiring dengan perkembangan teknologi informasi yang makin maju, aspek keamanan pada proses pertukaran informasi harus diperhatikan. Hal tersebut dikarenakan terdapat informasi atau data penting yang hanya boleh diakses oleh suatu perusahaan maupun sekolah tertentu [1]. Misalnya pada Sekolah Menengah Kejuruan Negeri (SMKN) 5 Semarang yang menggunakan e-Rapor untuk melakukan pertukaran informasi dalam merekap nilai dan mencetak rapor.

Pengisian e-Rapor dilakukan oleh guru SMKN 5 Semarang yang disimpan sementara di *server* sekolah. Kemudian dikirim kepada *server* Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbud). Proses pengiriman data ke *server* sekolah hanya dilakukan di jaringan sekolah menggunakan *router*. *Router* yang dapat mengakses jaringan tersebut yaitu *Router* 1 (Ruang Jurusan Teknik Komputer dan Jaringan serta Ruang Jurusan Teknik Pemesinan), *Router* 2 (Ruang Tata Usaha, Ruang Kurikulum, dan Rung Guru), dan *Router* 3 (Ruang Jurusan Teknik Komunikasi, Ruang Jurusan Teknik Kendaraan Ringan, Ruang Jurusan Desain Pemodelan dan Informasi Bangunan, Ruang Jurusan Listrik dan Ruang Kesiswaan). Jaringan di SMKN 5 Semarang menggunakan IP *Public*, namun keamanannya lemah sehingga SMKN 5 Semarang pernah mengalami peretasan khususnya pada e-Rapor. Maka dari itu dibutuhkan keamanan agar e-Rapor tersebut aman dan tidak diretas oleh *hacker*. Salah satu cara dalam menjamin keamanan proses pertukaran informasi yaitu menggunakan teknologi *Virtual Private Network* (VPN). VPN merupakan teknologi jaringan yang mengakses jaringan publik di mana ketika perangkat mengakses jaringan tersebut maka akan diarahkan ke jaringan pribadi [2]. VPN memiliki beberapa kelebihan yaitu pertukaran data antara pengirim dan penerima terenkripsi sehingga aman [3].

VPN dapat diimplementasikan menggunakan *tunneling* protokol. *Tunneling* protokol VPN tersebut dibagi menjadi *site to site access* VPN (SSL dan GRE) dan *remote access* VPN (PPTP, L2TP, MPLS). *Site to site access* VPN digunakan untuk menyatukan berbagai lokasi menjadi satu jaringan, sedangkan *remote access* VPN digunakan untuk mengatur atau mengendalikan *server* pada suatu jaringan [4][5].

Terdapat penelitian sebelumnya mengenai *tunneling* protokol VPN. Pada jenis *site to site access* VPN, *Secure Souckets Layer* (SSL) keamanannya rendah, performanya kurang baik ketika di bawah tekanan tinggi, dan tidak mendukung pada OS non-Windows. *Generic Routing Encapsulation* (GRE) sering mengalami keterlambatan terkirimnya data dan penggunaan aplikasi tidak lancar. Kemudian pada *remote access* VPN, L2TP lebih direkomendasikan daripada PPTP dan MPLS dari segi keamanan yang baik, kelancaran aplikasi dan pengiriman data, serta performa baik walaupun di bawah tekanan tinggi. PPTP melakukan enkripsi tradisional yang keamananya lemah. *Multiprotocol Label Switching* (MPLS) pengaturannya rumit, sangat tergantung pada *Internet Service Provider* (ISP), dan biasanya digunakan pada sistem yang besar [6]. Berdasarkan hal tersebut, penelitian ini menggunakan L2TP sebagai *tunneling* protokol VPN untuk mengakses e-Rapor SMKN 5 Semarang.

Struktur *paper* ini disusun sebagai berikut. Bagian II membahas metode yang diusulkan. Bagian III membahas konfigurasi L2TP dan konfigurasi *Windows Client*. Bagian

IV membahas dan menganalisis hasil penelitian. Bagian V menarasikan kesimpulan.

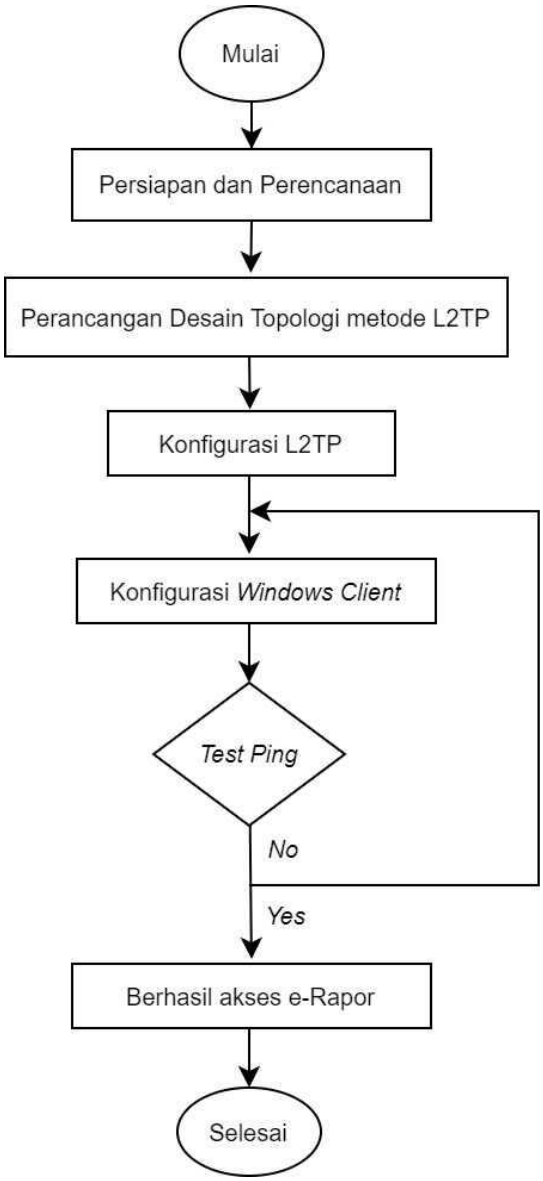
II. METODE YANG DIUSULKAN

Penelitian menggunakan PPDIOO (*Prepare, Plan, Design, Implement, Operate,* dan *Optimize*) sebagai metode perancangan jaringan. Jaringan SMKN 5 Semarang diaplikasikan *Virtual Private Network* (VPN) berdasarkan *Layer Two Tunneling Protocol* (L2TP). Pemilihan L2TP bertujuan untuk memudahkan guru mengakses e-Rapor SMKN 5 Semarang di mana saja dengan aman.

A. PPDIOO

PPDIOO merupakan metode perancangan jaringan yang dikembangkan oleh Cisco. Metode PPSIOO dapat memberikan infrastruktur jaringan yang adaptif [7][8]. Metode tersebut ditunjukkan pada Gambar 1 yang terdiri dari beberapa tahapan antara lain:

1. *Prepare* (persiapan)
   Persiapan dilakukan dengan pengumpulan data melalui observasi di SMKN 5 Semarang. Hasil observasi menunjukkan SMKN 5 Semarang belum menggunakan VPN pada jaringannya. Terdapat *router* yang dapat mengakses jaringan tersebut yaitu *Router* 1 (Ruang Jurusan Teknik Komputer dan Jaringan serta Ruang Jurusan Teknik Pemesinan), Router 2 (Ruang Tata Usaha, Ruang Kurikulum, dan Rung Guru), dan *Router* 3 (Ruang Jurusan Teknik Komunikasi, Ruang Jurusan Teknik Kendaraan Ringan, Ruang Jurusan Desain Pemodelan dan Informasi Bangunan, Ruang Jurusan Listrik dan Ruang Kesiswaan). Jaringan tersebut pernah mengalami kebobolan data oleh *hacker*, sehingga salah satu solusinya yaitu merancang L2TP VPN untuk mendapatkan keamanan pada proses pertukaran data informasi.
2. *Plan* (perencanaan)
   Perencanaan dilakukan dengan menganalisis kebutuhan yang digunakan pada perancangan L2TP dalam penelitian yang ditunjukkan pada Tabel 1. Device yang digunakan adalah MikroTik *routerboard* yang berfungsi sebagai *bandwidth management*, DHCP, DNS *server*, *hotspot server*, *proxy server*, dan *router* jaringan [9].
3. *Design* (desain)
   Desain dilakukan dengan mendesain topologi jaringan dengan konfigurasi L2TP sebagai *tunnel protocol* VPN yang diterapkan pada jaringan SMKN 5 Semarang. Desain topologi jaringan penelitian ini ditunjukkan pada Gambar 2. *Router* 1 bertindak sebagai *router server* sedangkan *router* 2 dan *router* 3 bertindak sebagai *router client*.

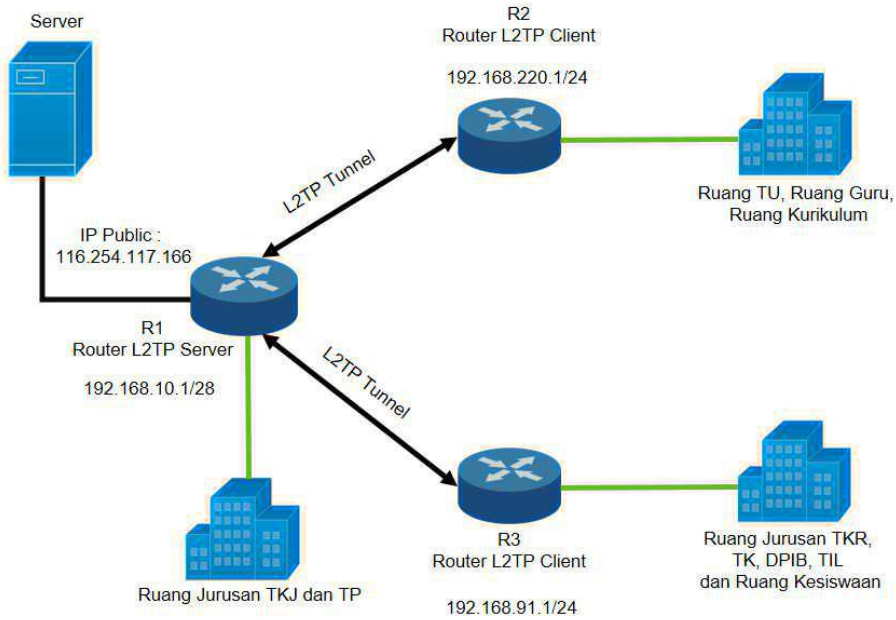


Gambar 1. Langkah Penelitian

Penggunaan metode L2TP (*Layer Two Tunneling Protocol*) harus mempunyai satu IP *Public* di *router server* agar konfigurasi dan akses dapat berjalan lancar. Alamat IP pada jaringan di Ruang Jurusan TKJ (Teknik Komputer dan Jaringan) dan Ruang Jurusan TP (Teknik Pemesinan) menggunakan alamat 192.168.10.1/24.

Tabel 1. Kebutuhan Penelitian

Device	IP Address
MikroTik RB1100AHx2	192.168.10.1/28
MikroTik RB 450G	192.168.10.1/24
MikroTik RB 450G	192.168.220.1/24



Gambar 2. Topologi Jaringan L2TP

Alamat IP pada jaringan di Ruang TU (Tata Usaha), Ruang Guru dan Ruang Kurikulum menggunakan alamat 192.168.220.1/24. Sedangkan alamat IP pada jaringan di Ruang Jurusan TK (Teknik Komunikasi), TKR (Teknik Kendaraan Ringan), DPIB (Desain Pemodelan dan Informasi Bangunan), TIL (Teknik Instalasi Listrik) menggunakan alamat 192.168.91.1/24. Pada *router server* menggunakan alamat IP *Public* 116.254.117.166 sebagai *Remote Address* yang akan memberikan IP *Address* ke *router client* secara otomatis.

4. *Implement* (implementasi)
   Implementasi L2TP digunakan untuk mengakses sistem aplikasi e-Rapor SMKN 5 Semarang. Implementasi dilakukan dari merancang atau merealisasikan desain topologi jaringan, dan konfigurasi L2TP pada jaringan. Konektivitas menggunakan *software utility* Winbox dan konfigurasi MikroTik menggunakan MAC *Address* atau protokol IP.
5. *Operate* (operasi)
   Pada tahapan ini, mengoperasikan jaringan L2TP untuk mengakses sistem aplikasi e-Rapor SMKN 5 Semarang. *Test ping* digunakan untuk menguji keberhasilan operasi jaringan tersebut.
6. *Optimize* (optimasi)
   Optimasi dilakukan ketika terdapat kendala pada jaringan maka dilakukan perbaikan agar dapat berjalan normal.

B. *Layer Two Tunneling Protocol*

Layer Two Tunneling Protocol (L2TP) adalah pengembangan dari Microsoft *Point-to-Point Tunneling Protocol* (PPTP) dan Cisco *Layer* 2 *Forwarding* (L2F) [10]. L2TP merupakan jenis *tunneling* protokol VPN yang terdiri dari beberapa VPN menjadi satu terowongan atau *tunnel* dengan mengedepankan keamanan melalui enkripsi data [11][12].

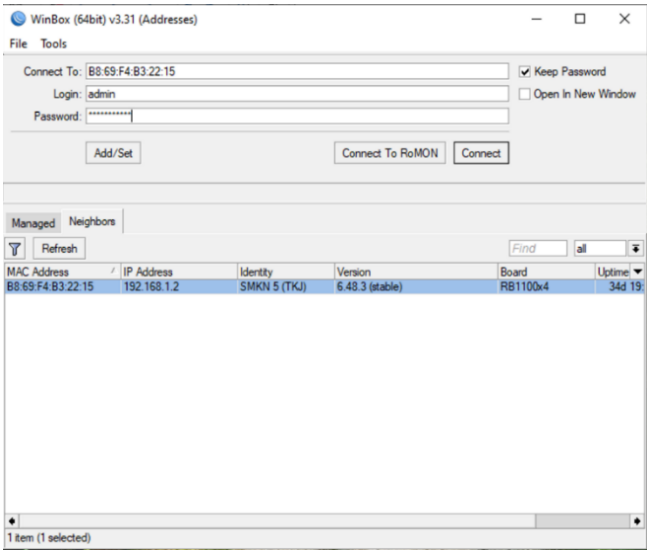
Layer Two Tunneling Protocol memiliki dua ujung komunikasi yaitu L2TP *Access Concentrator* (LAC) dan L2TP *Network Server* (LNS). LAC sebagai klien dan LNS sebagai *server* [13]. L2TP dapat didukung oleh *routed protocol* yang merupakan protokol jaringan yang dapat digunakan untuk mengirimkan data *user* dari *network* satu ke *network* lainnya. *Routed protocol* tersebut misalnya TCP/IP, IPX/SPX, AppleTalk, dan lain-lain [14]. L2TP dipilih sebagai *tunneling* protokol VPN pada penelitian ini karena proses pertukaran data terenkripsi sehingga aman.

III. KONFIGURASI L2TP DAN WINDOWS *CLIENT*

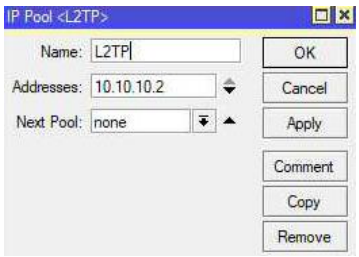
A. *Konfigurasi L2TP*

Konfigurasi L2TP diterapkan pada *router* secara bergantian dan dilakukan menggunakan aplikasi Winbox. Konfigurasi dilakukan di ruang *server* dimana SMKN 5 Semarang memiliki total *bandwidth* internet sebesar 190 Mbps. Konfigurasi dilakukan dengan beberapa tahapan sebagai berikut:

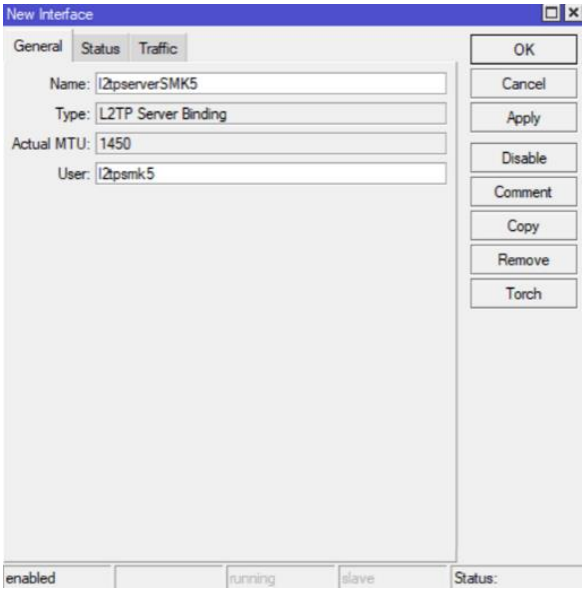
1. Mengkoneksikan *router*
   Router dikoneksikan ke aplikasi Winbox dengan memasukkan IP *Address router*, *username*, dan *password* kemudian *connect* seperti Gambar 3.
2. Membuat IP Pool L2TP
   IP Pool seperti yang ditunjukkan pada Gambar 4 merupakan salah satu fitur MikroTik untuk mendapatkan IP *Address* secara otomatis ketika melakukan koneksi ke *router server* [15].
3. Membuat *Interface* baru
   Membuat *interface* baru dilakukan dengan masuk ke tab PPP di menu utama WinBox kemudian pada tab *interface* klik *new interface*. Seperti Gambar 5 pada kolom *Name* diisi “l2tpserverSMK5” dan pada kolom *user* di isi “l2tpsmk5”.



Gambar 3. Login WinBox

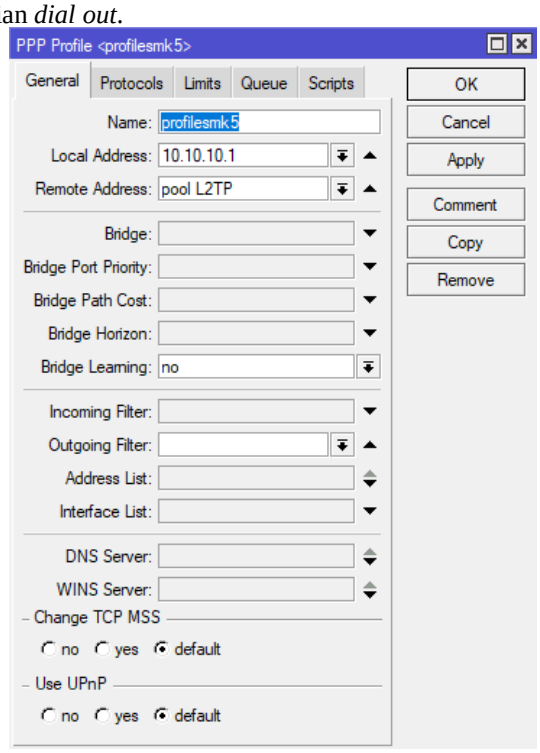


Gambar 4. IP *Pool* L2TP

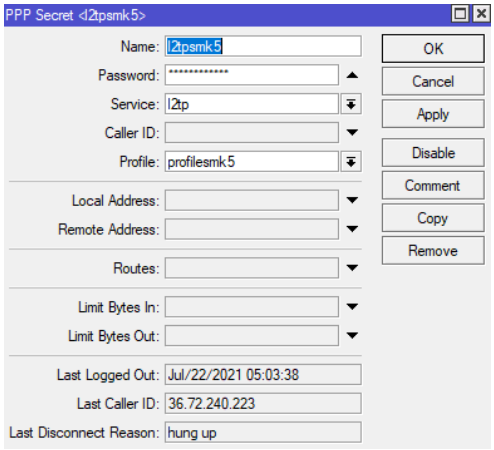


Gambar 5. *New Interface* L2TP

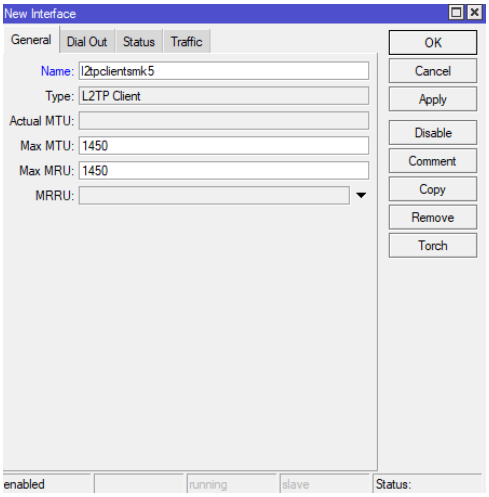
4. Membuat PPP *Profile*
   Pada *tab* PPP di menu utama WinBox pilih *profile* kemudian akan muncul seperti Gambar 6 kemudian klik tanda +. Pada kolom *Name* diisi dengan "profilesmk5", *Local Address* diisi sesuai pada *range* IP yang sudah dibuat pada IP *Pool*, dan *Remote Address* diisikan nama IP *Pool* tersebut.
5. Membuat PPP *Secret*
   PPP *Secret* seperti ditunjukkan pada Gambar 7 nantinya akan digunakan pada *router client* untuk dapat terhubung pada *router server*. Pada kolom name isikan "l2tpsmk5", lalu isi *password*, untuk *service* pilih "l2tp" dan *profile* pilih profil yang sudah dibuat "profilesmk5".
6. Konfigurasi *Dial Out*
   Tambah *interface* L2TP *Client* pada *router* R2, *name* diisi "l2tpclientsmk5" seperti Gambar 8. Kemudian agar dapat terkoneksi ke *router server*, maka masuk ke tab *dial out* isi kolom *Connect to* dengan IP *Public router server*. Kolom *user* dan *password* diisi PPP Secret yang telah dibuat di *router server* dapat dilihat pada Gambar 9 bagian *dial out*.



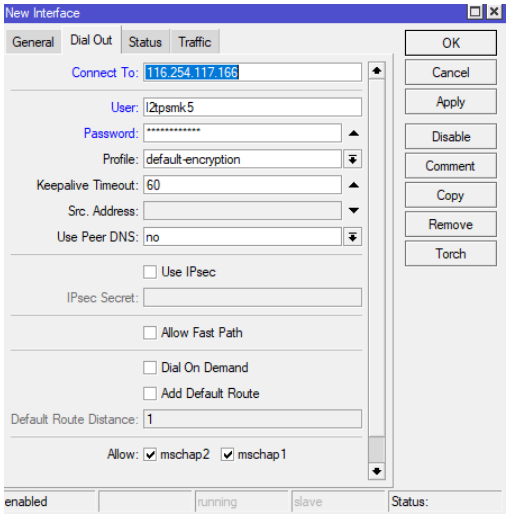
Gambar 6. PPP *Profile*



Gambar 7. PPP *Secret*



Gambar 8. *New Interface*

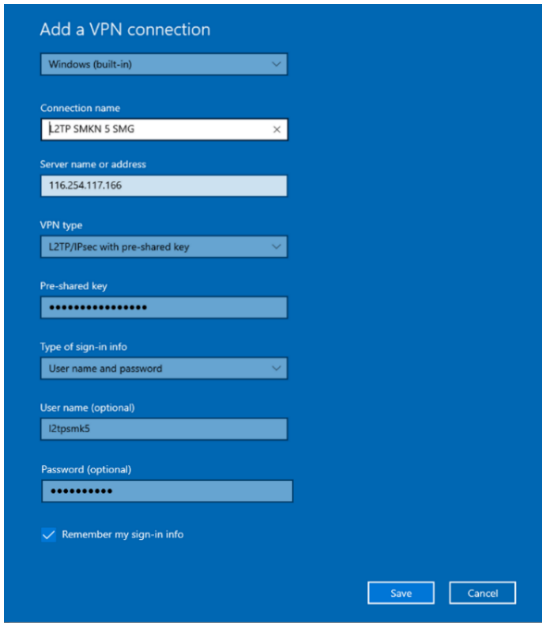


Gambar 9. Konfigurasi *Dial Out*

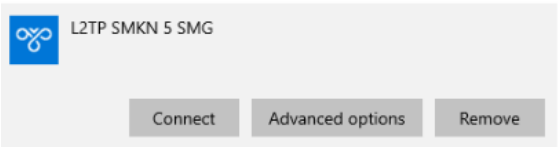
B. Konfigurasi Windows Client

Setelah konfigurasi L2TP, maka dilakukan konfigurasi *windows client*. Hal tersebut agar aplikasi e-Rapor dapat diakses. Berikut tahapan konfigurasi *windows client*:

1. Pada *settings devices* pilih network & internet. Kemudian *add a* VPN *connection* untuk menambahkan
2. VPN dan memulai konfigurasi hingga muncul seperti Gambar 10.
3. Pada kolom VPN Provider, pilih "Windows (*built-in*)" untuk kolom.
4. Pada kolom *connection name* diisi dengan "L2TP SMKN 5 SMG". *Server name or address* adalah IP *Public* yaitu 116.254.117.166.
5. Pada kolom VPN *type*, pilih "L2TP/IPSec *with pre-shared key*".
6. Pada kolom *Pre-shared key* masukan *pre-shared key* yang sama seperti di VPN (*Virtual Private Network*) *server*-nya.



Gambar 10. Penambahan VPN pada *Windows Client*



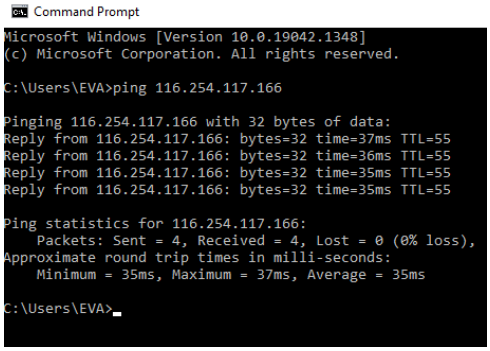
Gambar 11. VPN pada *Windows Client*

7. Pada kolom *type of sign-in info*, pilih "*user name* dan *password*".
8. Pada kolom *user name* diisi "l2tpsmk5" untuk *user name* VPNnya kemudian mengisi *password*.
9. Beri centang pada *remember my sign-in info* dan klik *save* untuk membuat koneksi. Jika telah berhasil maka akan muncul seperti Gambar 11.
10. Klik tombol *connect* agar tersambung dengan *Virtual Private Network* (VPN).

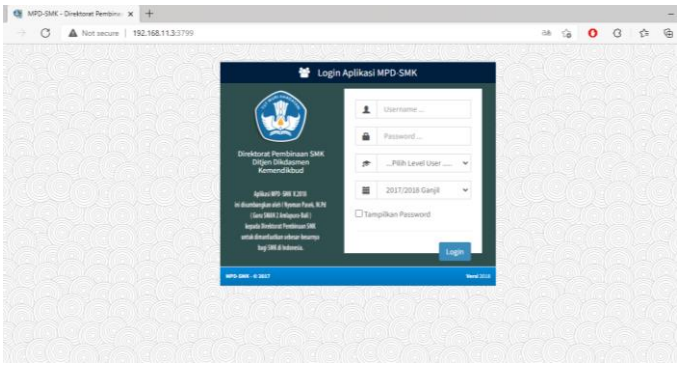
IV. HASIL DAN PEMBAHASAN

Penelitian dilakukan di jaringan SMKN 5 Semarang yang sebelumnya telah terdapat *router server* dan *router client* namun belum menggunakan teknologi *Virtual Private Network* (VPN). SMKN 5 Semarang menggunakan IP *Address* yang bersifat IP Publik yaitu 192.168.1.2. Tidak adanya *password* keamanan menyebabkan IP tersebut mudah diketahui banyak orang. Hal tersebut yang mengakibatkan data e-Rapor SMKN 5 Semarang pernah diretas.

Penelitian ini mengaplikasikan teknologi VPN dengan *tunneling protocol* menggunakan *Layer Two Tunneling Protocol* (L2TP). Pengujian atau *test ping* seperti Gambar 12 menunjukkan bahwa L2TP berhasil diterapkan.



Gambar 12. Test Ping L2TP



Gambar 13. Akses Aplikasi e-Rapor

Telah dilakukan pengujian akses aplikasi e-Rapor. Ketika ingin mengakses aplikasi e-Rapor, pengguna atau pihak guru harus tersambung VPN L2TP SMKN 5 Semarang dengan IP *Public* 116.254.117.166 pada *windows client* atau PC pengguna. Kemudian membuka dan mengetik 192.168.11.3:3799 pada tab browser maka akan muncul seperti Gambar 13 aplikasi e-Rapor SMKN 5 Semarang. Manfaat lain selain keamanan adalah guru dapat mengakses e-Rapor di mana saja.

V. KESIMPULAN

Penelitian mengaplikasikan teknologi VPN dengan *tunneling protocol* menggunakan *Layer Two Tunneling Protocol* (L2TP). Ketika ingin mengakses aplikasi e-Rapor, *windows client* harus tersambung VPN L2TP SMKN 5 Semarang dengan IP *Public* 116.254.117.166 pada *windows client* atau PC pengguna. Kemudian membuka dan mengetik 192.168.11.3:3799 pada tab browser untuk dapat mengakses aplikasi e-Rapor SMKN 5 Semarang. L2TP tersebut menyembunyikan IP *Address* yang bersifat IP Publik dan memberikan IP *Address port* untuk mengakses e-Rapor. Proses pertukaran data antara pengirim dan penerima juga terenkripsi, sehingga akan memberikan keamaan data dan terhindar dari serangan *hacker*. Manfaat lain selain keamanan adalah guru dapat mengakses e-Rapor tidak hanya pada jaringan SMKN 5 Semarang, namun di mana saja apabila terhubung internet.

DAFTAR ACUAN

[1] A. P. Pamungkas, Muhammad Reza Putra, and M. Hafizh, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko-muko," *J. KomtekInfo*, vol. 8, pp. 189–194, 2021, doi: 10.35134/komtekinfo.v8i3.143.

[2] S. Liu, T. Zeng, Y. Chao, and H. Wang, *Application of VPN Based on L2TP and User's Access Rights in Campus Network*, vol. 10989 LNAI. Springer International Publishing, 2018.

[3] A. Amarudin and S. D. Riskiono, "Analisis dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (VPN)," *J. Teknoinfo*, vol. 13, no. 2, p. 100, 2019, doi: 10.33365/jti.v13i2.309.

[4] F. Firmansyah, M. Wahyudi, and R. A. Purnama, "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP," *JUITA J. Inform.*, vol. 7, no. 2, p. 129, 2019, doi: 10.30595/juita.v7i2.4491.

[5] D. Irawan1 and Fatoni, "Penerapan IP Security pada Jaringan VPN Site to Site di PT. Pertamina Ubeb Adera Pengabuan," *Univ. Bina Darma*, 2018.

[6] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," *Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017*, pp. 39–44, 2017, doi: 10.1109/NSysS.2017.7885799.

[7] L. Hernandez *et al.*, *Optimization of a Wifi Wireless Network that Maximizes the Level of Satisfaction of Users and Allows The Use of New Technological Trends in Higher Education Institutions*, vol. 11587 LNCS. Springer International Publishing, 2019.

[8] M. Iqbal, N. N. P, M. Iqbal, M. Informatika, and P. N. Subang, "Perancangan dan Simulasi Jaringan Komputer Politeknik Negeri Subang Menggunakan Packet Tracer Versi 6.2 dengan Metode PPDIOO," *J. Ilm. Berk. TEDC*, vol. 14, no. 1, pp. 49–53, 2020.

[9] S. N. Khasanah and L. A. Utami, "Implementasi Failover Pada Jaringan WAN Berbasis VPN," *J. Tek. Inform.*, vol. 4, no. 1, pp. 62–66, 2018, [Online]. Available: https://ejournal.antarbangsa.ac.id/jti/article/view/190.

[10] E. Ramadhani, "Anonymity Communication VPN and Tor: A Comparative Study," *J. Phys. Conf. Ser.*, vol. 983, no. 1, 2018, doi: 10.1088/1742-6596/983/1/012060.

[11] N. S. Tarkaa, D. N. Nwabuike, and P. C. Lifu, "Design And Simulation Of Internet Virtual Private Network For Large Enterprise Using Riverbed Modeler," *Int. J. Res. Eng. anf Sci.*, vol. 6, no. 6, pp. 44–57, 2018, [Online]. Available: http://ijres.org/papers/Volume 6/Vol-Issue6/Version-1/F0606014457.pdf.

[12] D. Y. K. Sharma and C. Kaur, “The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 2336–2339, 2020, doi: 10.35940/ijrte.f8335.038620.

[13] D. M. Ajay and E. Umamaheswari, “Packet Encryption for Securing Real-Time Mobile Cloud Applications,” *Mob. Networks Appl.*, vol. 24, no. 4, pp. 1249–1254, 2019, doi: 10.1007/s11036-019-01263-1.

[14] Q. Wang *et al.*, “Exploration and Practice of Complex Teaching Cases Based on Campus Network,” in *International Conference on Education, Management, Computer and Society*, 2020, pp. 349–357, doi: 10.38007/proceedings.0001812.

[15] D. Ruwaida and D. Kurnia, “Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di Smk Dwiwarna,” *Comput. Eng. Sci. Syst. J.*, vol. 3, no. 1, p. 45, 2018, doi: 10.24114/cess.v3i1.8267.