ISSN: 2477-5126
e-ISSN:2548-9356

MERANCANG DAN IMPLEMENTASI VPN PPTP UNTUK KONEKSI CLIENT SERVER APLIKASI KEUANGAN IFAS
(Studi Kasus Pada Yayasan Teratai Putih Global)

Masroni[1*)], Atit Pertiwi[2], Amat Suroso[3]
[1]Program Studi Magister Manajemen Sistem Informasi, Universitas Gunadarma, Depok
[2]Program Studi Magister Manajemen Sistem Informasi, Universitas Gunadarma, Depok
[3]Sistem informasi, STMIK Bani Saleh, Bekasi
[1]Jln. Masrgonda Raya, Kota Depok, 16424, Indonesia
[2] Jln. Masrgonda Raya, Kota Depok, 16424, Indonesia
[3]Jl. M.Hasibuan No. 68, Kota Bekasi, 50272, Indonesia
email: [1]masroni.alamsyah@gmail.com, [2]atit@staff.gunadarma.ac.id, [3]ahmad_suroso04@yahoo.com

***Abstract* – The Teratai Putih Global Foundation is an institution engaged in the field of education which has 9 (nine) school units from Islamic preschool, Islamic Elementary School, Islamic Junior High School, Islamic High School and Vocational Schools spread across Bekasi and Jakarta. The data collection process is mainly related to the administrative and financial processes of students and the recording of school financial cash flows. The foundation and the nine units have school administration system software IFAS (Integrated Finance and Accounting System) in their respective school units, this condition makes it difficult for the foundation to consolidate data and daily reports in real time because they are not connected to each other. VPN (Virtual Private Network) technology allows anyone to be able to access the local network from outside using the internet. The purpose of using a VPN is so that users can access the resources on the server, connect to the database server in real time and get the same rights and settings as physically in the place where the local network is located. With the NDLC (Network Development Life Cycle) method, a method for designing and building networks, VPN connections are designed for a client-server topology and successfully implemented for the IFAS program to run well and smoothly.**

***Abstrak* – Yayasan Teratai Putih Global adalah Lembaga yang bergerak di bidang pendidikan yang memiliki 9 (Sembilan) unit sekolah mulai dari KB/TK Islam, SD Islam, SMP Islam, SMA Islam serta SMK yang tersebar di Bekasi dan Jakarta. Dalam proses pendataan terutama berkaitan dengan proses administrasi dan keuangan siswa serta pencatatan arus kas keuangan sekolah. Yayasan dan kesembilan unit tersebut memiliki perangkat lunak sistem administrasi sekolah IFAS (*Integreted Finance and Accounting System*) pada unit sekolah masing-masing, kondisi ini menyulitkan pihak yayasan dalam proses konsolidasi data dan laporan harian secara realtime karena antar satu dengan yang lain tidak saling terhubung. Teknologi VPN (Virtual Private Network) memungkinkan setiap orang untuk dapat mengakses jaringan lokal dari luar menggunakan internet. Tujuan menggunakan VPN adalah agar user dapat mengakses sumber daya yang ada pada server, terkoneksi ke data base server secara *real time* dan mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Dengan metode NDLC *(Network Development Life Cycle)* sebuah metode dalam merancang dan membagun jaringan, koneksi VPN dirancang untuk topologi *client-server* dan berhasil diimplementasikan untuk program IFAS dapat berjalan dengan baik dan lancar.**

***Kata Kunci* – VPN, sekolah, perangkat lunak, keuangan, NDLC**

*) **penulis korespondensi**: Masroni
Email: masroni.alamsyah@gmail.com

I. PENDAHULUAN

Yayasan Teratai Putih Global yang berlokasi di Kota Bekasi berdiri sejak tahun 1979 yang bergerak dalam bidang pendidikan. Saat ini Yayasan Teratai Putih Global menaungi sembilan sekolah dengan tingkatan yang berbeda. Delapan unit sekolah berada di Kota Bekasi dengan lokasi yang berbeda-beda. KB/TK Islam, SD Islam, SMP Islam dan SMA Islam Teratai Putih Global berada di daerah Cimuning, SMK Teratai Putih Global 1 lokasinya di perumahan Bumi Satria Kencana Kec. Jakasampurna, SMK Teratai Putih Global 2 berlokasi di Perumnas 1 Kayuringin Jaya, SMK Teratai Putih Global 3 dan SMK Teratai Putih Global 4 berlokasi di daerah ciketing serta SMK Teratai Putih Jakarta yang berlokasi di Perumnas Klender Jakarta Timur.

Yayasan Teratai Putih Global mengembangkan sebuah perangkat lunak untuk mendukung kegiatan administrasi yang berkaitan dengan data pegawai, siswa serta keuangan baik pada sisi sekolah maupun Yayasan, dimana aplikasi ini dapat berjalan pada komputer desktop atau laptop secara lokal maupun jaringan *client-server*. Aplikasi ini dinamakan IFAS *(Integreted Finance and Accounting System)* yang menerapkan prinsip penggabungan aktivitas *finance* dan *accounting* dalam sebuah aplikasi.

Gbr. 1 tampilan login aplikasi IFAS

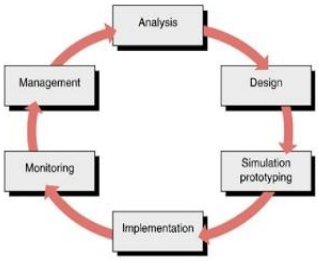
Gambar 1 memperlihatkan tampilan login aplikasi IFAS pda Yayasan Teratai Putih Global, pada saat Yayasan ingin melakukan integrasi data dari sembilan unit sekolah, terjadi hambatan karena lokasi masing-masing sekolah yang jaraknya berjauhan serta jumlah data yang begitu banyak dan masing-masing sekolah menggunakan koneksi internet dari penyedia layanan yang berbeda, sementara jika ingin beralih koneksi internet dari sembilan sekolah dan yayasan ke penyedia layanan internet yang sama akan membutuhkan waktu yang lama dan biaya yang besar. Dalam penelitian ini, peneliti mengimplementasikan teknologi VPN yang terdapat pada fitur perangkat *router* Mikrotik sebagai solusi permasalahan tersebut. VPN *(Virtual Prtivate Network)* adalah salah satu teknologi koneksi jaringan yang dapat terkoneksi dengan jaringan lain yang berbeda segmen dengan sebuah jalur pribadi dalam jaringan publik (internet) yang telah dibentuk jalurnya seakan-akan terhubung secara *point to point* dimana data melewati jarigan public dan dapat mencapai tujuan akhir [1]. Melalui koneksi VPN inilah *client* sekolah dimana terdapat aplikasi keuagan IFAS dapat terhubung dengan komputer server yang terdapat di Yayasan sebagai pusat penampungan data pada aplikasi IFAS. Tujuan penelitian ini adalah mengimplementasikan teknologi VPN sebagai solusi bagi Yayasan Taratai Putih Global (kantor pusat) agar dapat mengintegrasikan data aplikasi yang terdapat pada sembilan sekolah (komputer *client*) yang berbeda lokasi dengan penyedia layanan internet yang berbeda [2]. Jaringan VPN di konfigurasi pada sebuah perangkat router Mikrotik RB750. Menurut Supendar [3] Mikrotik adalah sebutan pada perangkat dari sebuah perusahaan produsen router yang telah berhasil memproduksi router yang handal, mikrotik teridiri dari 2 macam yaitu: perangkat keras (Mikrotik Router Board) dan perangkat lunak/ sistem operasi (Mikrotik Router OS) yang berbasis LINUX yang dapat diinstal pada komputer standar yang memiliki spesifikasi seperti router. Mikrotik router dapat dikonfigurasi dengan mode grafis untuk memudahkan administrator menggunakan aplikasi winbox [4].

II. PENELITIAN YANG TERKAIT

Penelitian terkait yang sebelumnya pernah dilakukan antara lain Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang [5], pada penelitian tersebut VPN berhasil diimplementasikan dan dapat menghubungkan antara kantor pusat dan kantor cabang menggunakan protokol VPN PPTP serta pertukaran data dapat dilakukan menggunakan aplikasi hamaci. Pada penelitian yang dilakukan oleh Lia Umaroh dan Machsun Rifaudin [6], berhasil mengimplementasikan VPN di perpustakaan Universitas Islam Malang untuk mempermudah dan mempercepat koneksi internet, VPN juga digunakan untuk melindungi privasi data agar lebih aman dan terlindungi. Pada penelitian Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP [7], berhasil mengimplementasikan VPN pada perusahaan dengan biaya relatif lebih murah dan tidak perlu melakukan investasi yang mahal, meskipun pada aspek keamanan protokol EoIP tidak melakukan enkripsi data, tetapi admin dapat melakukan monitoring pada *interface* EoIPnya serta mengaktifkan fitur *firewall/filtering.*

III. METODE PENELITIAN

Penelitian ini menggunakan metode NDLC (*Network Development Life Cycle).* Metode NDLC digunakan dalam merancang dan implementasi sebuah infrastruktur jaringan dengan tahapan-tahapan antara lain *analysis, design, simulation prototyping, implementation, monitoring* dan *management* [8], seperti yang ditunjukkan pada Gbr. 2



Gbr. 2 tahapan *network development life cycle*

Gambar 2 menujukkan siklus tahapan pada NDLC *(network development life cycle)* yang sering digunakan dalam merancang sebuah koneksi jaringan.

A. *Analysis*

Tahapan pertama adalah melakukan analisa kebutuhan baik dari sisi pengguna maupun perangkat yang dibutuhkan, analisa permasalahan yang terdapat di lokasi, analisa keinginan dan rencana dari pengguna, serta analisa desain topologi jaringan yang sudah ada saat ini [9]. Pada tahap ini dapat dilakukan dengan cara:

1. Wawancara pihak terkait mulai dari struktur organisasi atas sampai ke level bawah atau operator agar mendapatkan data yang dibutuhkan.
2. Survei langsung kelapangan dengan mendatangi lokasi yang akan dibangun jaringan VPN untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain.
3. Membaca buku manual dari dokumentasi yang mungkin pernah dibuat sebelumnya. Dokumentasi data profil pengguna, pengalamatan, aturan-aturan, skema, desain rancangan, spesifikasi perangkat dan lain sebagainya yang sudah ada.
4. Mempelajari dengan seksama setiap data yang didapat dari data-data sebelumnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahapan ini adalah:
   - *User/people*: jumlah pengguna, *user profile*, kegiatan yang sering dilakukan, kategori pengguna yang ada, level teknis pengguna dan otorisasi pengguna.
   - Media *hardware* dan *software*: peralatan yang sudah ada, status jaringan terkini, nomor seri perangkat, ketersedian data yang dapat diakses dari peralatan, aplikasi *software* yang digunakan.
   - *Data*: jumlah *client* yang dilayani, jumlah inventaris sistem, keamanan sistem yang sudah ada untuk menjamin keamanan data.
   - *Network*: desain jaringan, konfigurasi, volume trafik jaringan, protokol, *network monitoring* yang ada saat ini, keinginan dan rencana pengembangan ke depan
   - Perencanaan fisik: kelistrikan, tata letak, ruang khusus, proteksi keamanan, dan kemungkinan akan pengembangan kedepan.

B. *Design*

Setelah memperoleh data pada tahapan analisis, pada tahap *design* ini adalah membuat gambar desain topologi jaringan interkoneksi jaringan yang akan dibangun. Dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang diinginkan. Desain bisa berupa desain struktur topologi, alur akses data, desain layout pengkabelan, dan sebagainya yang akan menggambarkan dengan jelas tentang proyek yang akan dibangun.

C. Simulation Prototyping

Pada tahap ini jaringan yan akan dibuat perlu dirancang dalam bentuk simulasi dengan bantuan aplikasi khusus di bidang *network* seperti GNS3, Packet Tracer, Netsim, Visio dan sebagainya [10]. Simulasi ini bertujuan untuk melihat kinerja awal dari rancangan jaringan yang akan dibangun dan sebagai bahan diskusi dengan tim yang lain.

D. Implementation

Pada tahapan ini pekerja jaringan akan menerapkan semua yang telah di analisis, direncanakan, didesain dan dismulasikan sebelumnya. Tahap implementasi ini akan memakan waktu yang lebih lama dari tahapan sebelumnya karena tahap ini dilakukan mulai dari menyiapkan alat dan bahan, instalasi, konfigurasi, testing, memastikan kestabilan serta keamanan dari jaringan yang dibuat.

E. Monitoring

Setelah melakukan implementasi jaringan tahapan selanjutnya adalah melakukan monitoring pada agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis, maka perlu dilakukan sebuah monitoring. Kegiatan monitoring dengan melakukan pengamatan pada:

1. Infrastruktur *hardware*: dengan mengamati kondisi *reliability*/ kehandalan sistem yang telah dibangun (*reliability = performance+availability+security*);
2. Memperhatikan jalannya paket data di jaringan (waktu, *latency*, *peektime*, *troughput* dan *traffic*);
3. Metode apa yang dipakai untuk mengamati kondisi jaringan dan komunikasi data secara umum, terpusat atau tersebar;
4. Pendekatan yang paling sering dilakukan adalah pendekatan *Network Management*. Pendekatan ini memungkinkan banyak perangkat baik yang lokal dan tersebar dapat dimonitor secara keseluruhan.

F. Management

Pada tahapan manajemen, yang perlu menjadi perhatian khusus adalah masalah kebijakan *(policy)* pada hasil rancang bangun jaringan. Kebijakan perlu dibuat untuk membuat/ mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung untuk jangka waktu yang lama dan unsur *reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level manajemen dan strategi bisnis perusahaan tersebut.

IV. HASIL DAN PEMBAHASAN

A. Analysis

Yayasan Teratai Putih Global mengalami kendala pada saat konsolidasi data antara pihak Yayasan dan sembilan sekolah karena menggunakan penyedia layanan internet yang berbeda. Dari hasil analisis instalasi jaringan VPN memerlukan beberapa alat dan bahan berikut ini :

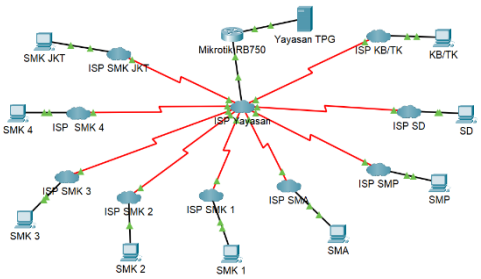
TABEL I
KEBUTUHAN ALAT DAN BAHAN

No	Alat/ bahan	Fungsi	Jumlah
1	Router Mikrotik RB750	Mengelola jaringan	1 pcs
2	Kabel UTP	Media Transmisi	2 pcs
3	Konektor RJ-45	Penghubung kabel ke *interface*	4 pcs
4	Koneksi Internet Static	Penghubung ke jalur public	1

Tabel 1 merupakan daftar alat dan bahan yang diperlukan untuk membuat jaringan VPN. Alat dan bahan tersebut diletakkan pada lokasi komputer server yang berada di Yayasan/ kantor pusat yang nantinya akan diinstalasi dan dikonfigurasi agar komputer *client* yang ada di sekolah dapat terhubung ke komputer server.

B. Design

Dalam membangun jaringan VPN diperlukan desain rancangan/ topologi yang akan digunakan. Topologi ini diperlukan agar memudahkan dalam proses instalasi dan penempatan alat serta melihat gambaran jalur koneksi antara yayasan dan sembilan sekolah.



Gbr. 3 desain topologi jaringan VPN Yayasan TPG

Gambar 3 memperlihatkan sebuah rancangan desain sebagai gambaran awal jaringan VPN yang akan dibangun di kantor Yayasan Teratai Putih Global dengan sembilan sekolah yang berada di lokasi berbeda dan memiliki sambungan internet dari penyedia layanan internet yang berbeda.

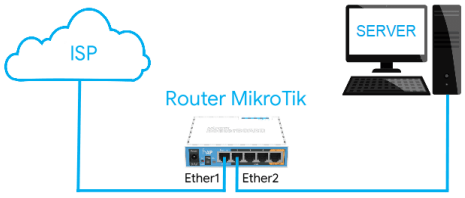
C. Simulation Protyping

Simulai dapat dilakukan dengan aplikasi *virtual machine*

D. Implementation

Pada tahap implementasi, ada beberapa langkah yang harus dikerjakan yaitu :

1. Membuat dua buah kabel LAN yang dibuat dari kabel UTP dengan tipe *straight* dimana kabel LAN ini digunakan untuk menghubungkan perangkat seperti tampak pada Gbr. 4 berikut ini :

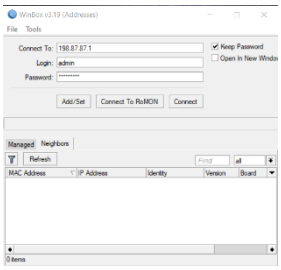


Gbr. 4 penyambungan kabel LAN pada perangkat

Gambar 4 menunjukkan dua buah kabel lan dimana satu kabel menghubungkan dari modem ISP ke router mikrotik dan satu kabel lagi dari router mikrotik ke komputer server.

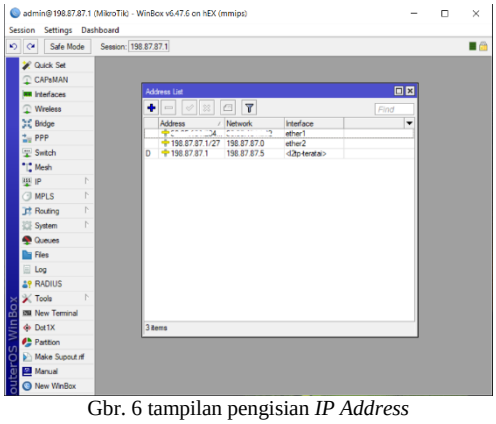
ISSN: 2477-5126
e-ISSN:2548-9356

2. Konfigurasi Mikrotik dengan mode grafis menggunakan aplikasi winbox, konfigurasi ini meliputi login ke perangkat router, pengisian *IP Address*, pembuatan *IP Pool*, aktivasi protokol VPN, pembuatan *profile*, pembuatan *security*, dan seting *rule* pada *firewall NAT* seperti yang diperlihatkan pada Gbr. 5, Gbr. 6, Gbr. 7, Gbr. 8, Gbr. 9, Gbr. 10, Gbr. 11 dan Gbr. 12.



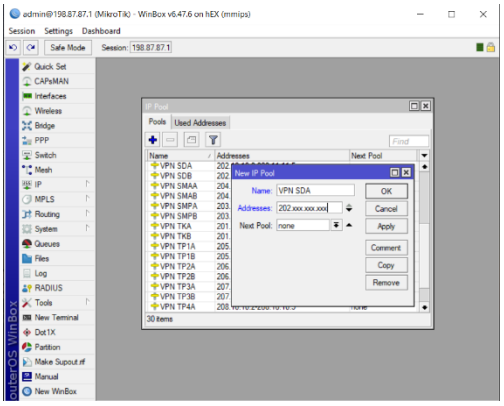
Gbr. 5 tampilan login router mikrotik menggunakan winbox

Gambar 5 adalah tampilan awal aplikasi winbox yang digunakan untuk mengakses perangkat mikrotik router dengan mode grafis dengan mengisikan *ip address* Mikrotik router serta data *user login* dan *password*.



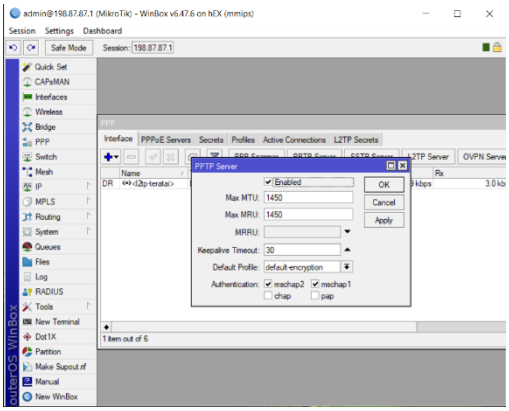
Gbr. 6 tampilan pengisian *IP Address*

Gambar 6 adalah menu untuk mengisikan *ip address* sesuai *ip address* yang telah ditetapkan sebelumnya.



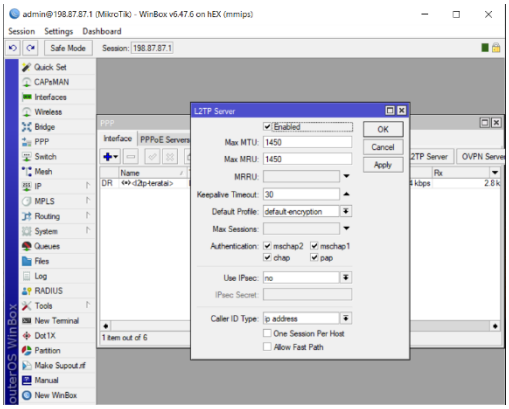
Gbr. 7 tampilan pembuatan *IP Pool*

Pada Gambar 7 memperlihatkan pembuatan *IP Pool* yang fungsinya untuk membentuk alamat dengan segment yang sama pada VPN *client*.



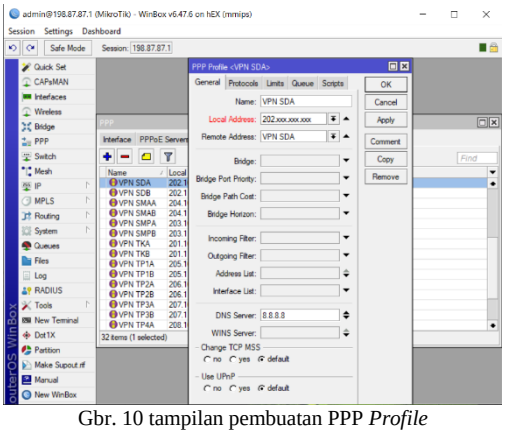
Gbr. 8 tampilan mengaktifkan protokol VPN PPTP

Gambar 8 adalah langkah untuk mengaktifkan protokol VPN PPTP dengan cara memberikan tanda centang pada pilihan *enable* lalu klik *apply* dan *ok*



Gbr. 9 tampilan mengaktifkan protokol VPN L2TP

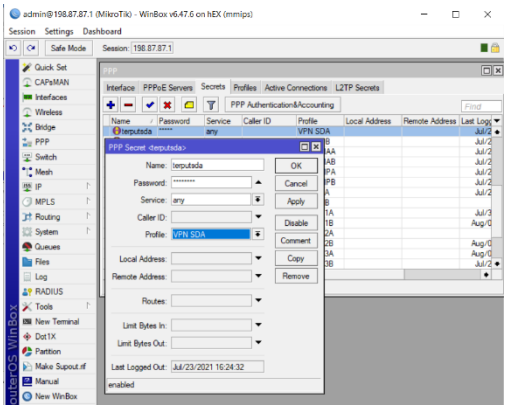
Gambar 9 adalah langkah untuk mengaktifkan protokol VPN L2TP dengan cara memberikan tanda centang pada pilihan *enable* lalu klik *apply* dan *ok.* Berbeda dengan protokol PPTP, protokol VPN L2TP telah menerapkan enkripsi data pada saat sistem akan melakukan transmisi data, sehingga pertukaran data menjadi lebih aman.



Gbr. 10 tampilan pembuatan PPP *Profile*

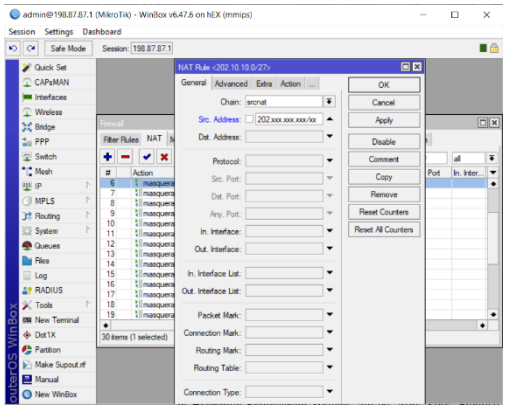
Langkah berikutnya pada gambar 10 adalah membuat profil VPN meliputi pemberian nama VPN, *local address* yang dituju dan remote address mengikuti IP Pool yang telah dibuat pada tahap sebelumnya pada Gbr.7

ISSN: 2477-5126
e-ISSN:2548-9356



Gbr. 11 tampilan pembuatan PPP *Secret*

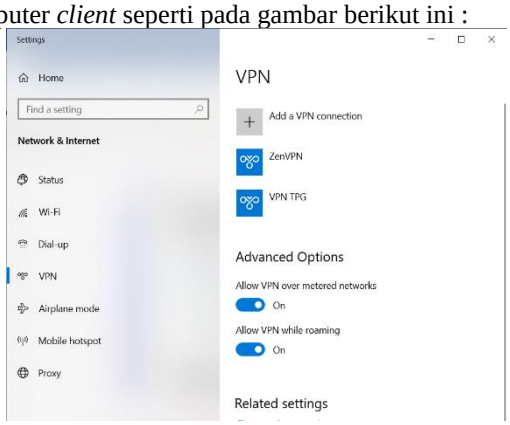
Gambar 11 adalah pembuatan PPP *secret* yang berfungsi sebagai otorisasi user pada saat melakukan koneksi VPN dimana terlebih dahulu terdapat autentikasi *username* dan *password* sebagai jaminan kemanan dan koneksi yang dapat dipercaya.



Gbr. 12 tampilan pembuatan *rule firewall NAT*

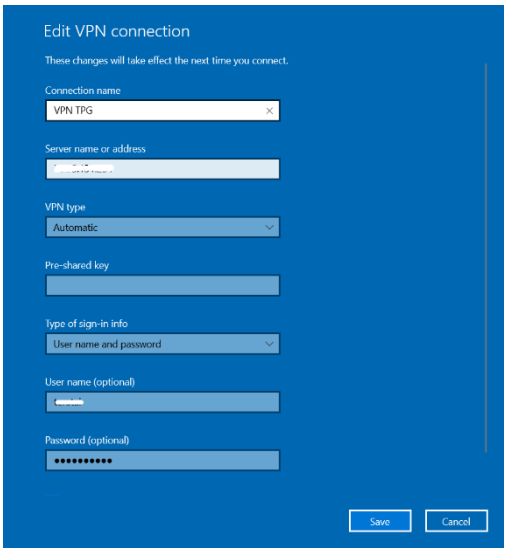
Langkah terakhir konfigurasi VPN adalah pembuatan rule untuk mengizinkan permintaan koneksi yang masuk untuk mencari sumber alamat yang diinginkan, sehingga setelah ditemukan, koneksi VPN dapat terbentuk seperti yang diperlihatkan pada gambar 12.

3. Setelah melakukan seting VPN pada router mikrotik, dilanjutkan dengan konfigurasi VPN pada komputer *client*. Konfigurasi VPN pada komputer *client* dapat dilakukan pada aplikasi VPN *client* atau bisa juga dengan fitur VPN yang telah tersedia pada sistem operasi yang digunakan. Langkah-langkah konfigurasi VPN pada komputer *client* seperti pada gambar berikut ini :



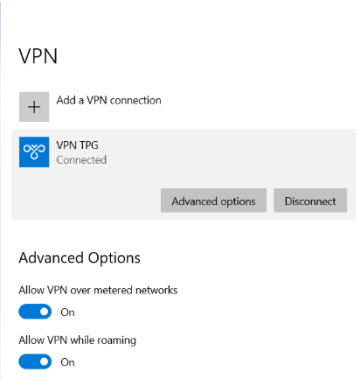
Gbr. 13 tampilan fitur VPN pada sistem operasi windows 10

Gambar 13 memperlihatkan fitur VPN yang terdapat pada sistem operasi windows 10 yang telah tersedia tanpa menginstal aplikasi tambahan, untuk menambahkan koneksi VPN pada komputer *client* ke komputer server bisa memilih opsi *Add a VPN Connection* dan lakukan beberapa seting seperti tampak pada gambar berikut ini :



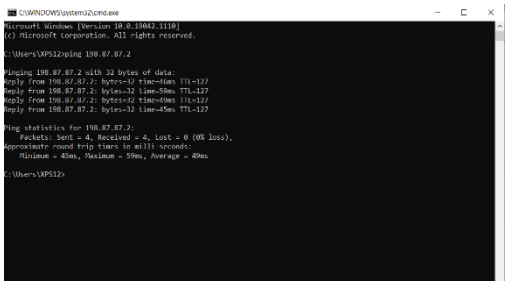
Gbr. 14 tampilan seting VPN pada sistem operasi windows 10

Gambar 14 menampilkan beberapa parameter yang harus diisi untuk membuat koneksi VPN agar terhubung ke komputer server. Selanjutnya klik *save* dan *connect* maka akan tampak seperti gambar berikut ini :



Gbr. 15 koneksi VPN sudah terhubung

Gambar 15 menampilkan status VPN *connected* menandakan koneksi VPN sudah terhubung dari komputer *client* ke komputer server. Untuk memastikan bahwa komputer *client* sudah terhubung ke komputer server, dapat diuji dengan melakukan test ICMP menggunakan *command prompt* seperti yang diperlihatkan pada gambar berikut :



Gbr. 16 *test* ICMP pada ke komputer server

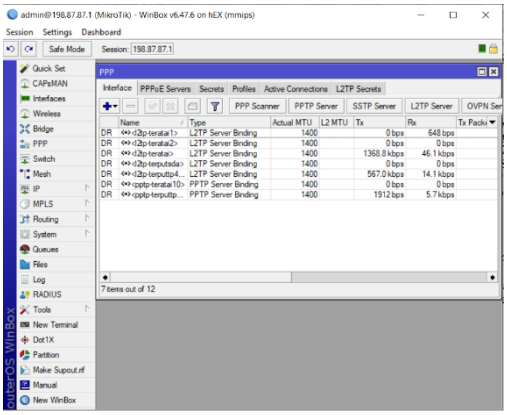
Gambar 16 menunjukkan *test* ICMP ke komputer server berhasil. Setelah koneksi *test* uji koneksi VPN berhasil langkah berikutnya adalah menjalankan aplikasi IFAS pada komputer client seperti yang diperlihatkan pada gambar di bawah ini :

Gbr. 17 aplikasi IFAS berhasil dijalankan

Gambar 17 menunjukkan aplikasi IFAS berhasil dijalankan pada komputer *client* dengan koneksi ke data base server yang ada di Yayasan Teratai Putih Global sehingga aplikasi IFAS ini dapat digunakan di sembilan sekolah melalui koneksi VPN yang telah dibentuk.

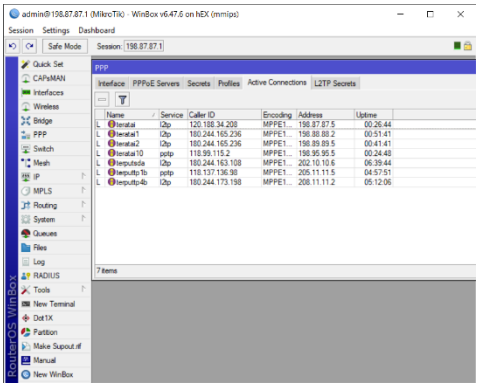
E. Monitoring

Proses monitoring pada jaringan VPN yang telah terhubung dapat dilakukan pada router mikrotik. Roter Mikrotik sudah dilengkapi dengan fitur untuk melakukan proses monitoring sesuai kebutuhan sehingga memudahkan administrator jaringan untuk memantau jalannya koneksi. Monitoring VPN pada router mikortik dapat dibuka pada menu PPP seperti yang ditunjukkan pada gambar berikut ini :



Gbr. 18 monitoring *traffic* pada setiap *interface* VPN yang aktif

Gambar 18 adalah tampilan monitoring yang dilakukan untuk memantau *traffic* / lalu lintas data yang terjadi pada *interface* VPN yang sedang aktif. *Traffic* yang dimonitor antara lain berkaitan dengan protokol VPN yang terbentu serta kondisi data transfer *upload* dan *download*. *Monitoring* juga dapat dilakukan dengan memantau *active connection* yaitu *user* siapa saja yang sedang aktif terhubung pada jalur VPN ke komputer server sehingga dapat memastikan *user* yang terhubung adalah *user* yang dikenali dan diberi akses untuk terhubung ke jalur VPN seperti diperlihatkan pada Gbr. 19 berikut :

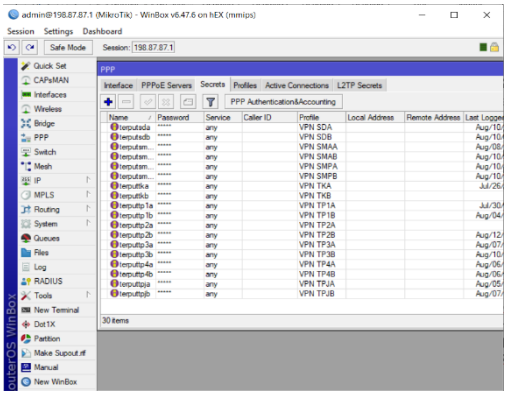


Gbr. 19 *monitoring* pada *user* yang sedang aktif

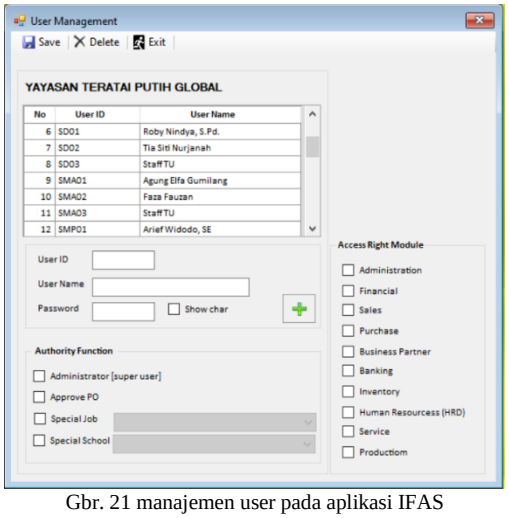
Gambar 19 menunjukkan *user* yang sedang aktif terhubung pada jaringan VPN ke komputer server, pada gambar tesebut dapat dilihat protokol *service* VPN apa yang sedang digunakan, sumber koneksi dari alamat mana serta durasi waktu koneksi sejak dihubungkan.

F. Management

Pada tahap manajemen ini, Yayasan Teratai Putih Global mengambil kebijakan bahwa tidak semua komputer *client* di sekolah dapat terhubung ke komputer server di Yayasan menggunakan koneksi VPN. Yayasan Teratai Putih Global hanya mengizinkan kepala Tata Usaha dan bagian kasir saja yang diberikan akses baik akses untuk koneksi VPN maupun akses masuk ke aplikasi IFAS. Manajemen user VPN dan user aplikasi IFAS data dilihat pada Gbr. 20 dan Gbr. 21 berikut ini :



Gbr. 20 manajemen user pada koneksi VPN



Gbr. 21 manajemen user pada aplikasi IFAS

V. KESIMPULAN

Berdasarkan hasil implementasi jaringan VPN pada Yayasan Teratai Putih Global untuk integrasi data base pada aplikasi IFAS dapat di simpulkan sebagai berikut :

1. Rancang bangun koneksi VPN pada Yayasan Teratai Putih Global berhasil dilakukan.
2. Komputer *client* pada sembilan sekolah berhasil terhubung ke komputer server yang berada di Yayasan menggunakan jalur VPN.
3. Aplikasi IFAS dapat dijalankan pada komputer *client* dengan mengakses data base pada komputer server.
4. Monitoring *user* pada jaringan VPN dapat dilakukan dengan memantau *traffic data* yang berjalan baik *upload* maupun *download*.
5. Manajemen *user* pada aplikasi IFAS telah dibuat untuk membatasi pengguna dan menjamin keamanan aplikasi serta data base.

Pada penelitian ini telah berhasil mengimplementasikan jaringan VPN untuk koneksi *client* server dengan menggunakan perangkat dan fitur standar yang terdapat pada Mikrotik. Untuk pengembangan dan penelitian berikutnya penulis menyarankan untuk meneliti dengan menggunakan perangkat lain yang lebih handal seperti CISCO atau Fortiget.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak Yayasan dan sekolah yang telah membantu menyediakan fasilitas dan sarana serta prasarana dalam penelitian ini dalam mengimplementasikan jaringan VPN untuk koneksi client server yang aman dan efisien.

DAFTAR PUSTAKA

[1] A. Setiawan, H. Priyanto and M. A. Irwansyah, "PERANCANGAN DAN IMPLEMENTASI VIRTUAL PRIVATE NETWORK DENGAN PROTOKOL PPTP PADA CISCO ROUTER 2901 (STUDI KASUS PRODI TEKNIK INFORMATIKA UNTAN)," *Jurnal Sistem dan Teknologi Informasi,* vol. 4, no. 2, 2016.

[2] Maharani and . F. Latifah, "Penerapan Teknologi Virtual Private Network Pada Wan PT. Asuransi Jiwa Tugu Mandiri Jakarta," *ndonesian Journal on Networking and Security,* vol. 7, no. 2, 2017.

[3] H. Supendar, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," *Bina Insani ICT Journal,* vol. 3, no. 1, 2016.

[4] Athailah, Mikrotik Untuk Pemula, Jakarta: MediaKita, 2013.

[5] S. Watmah, "Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang," *INSANTEK – Jurnal Inovasi dan Sains Teknik Elektro,* vol. 1, no. 1, 2020.

[6] L. Umaroh and M. Rifauddin, "Implementasi Virtual Private Network (VPN) Di Perpustakaan Universitas Islam Malang," *BACA: Jurnal Dokumentasi dan Informasi,* vol. 42, no. 2, 2020.

[7] H. Kuswanto, "Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP," *Paradigma: Jurnal Komputer dan Informatika,* vol. 19, no. 1, 2017.

[8] H. Kurniawan and S. Kosasi, "Penerapan Network Development Life Cycle Dalam Perancangan Intranet Untuk Mendukung Proses Pembelajaran," *Jurnal Ilmiah SISFOTENIKA,* vol. 5, no. 2, 2015.

[9] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *Jurnal Mahasiswa Bina Insani,* vol. 4, no. 1, 2019.

[10] Iskandar, Buku Ajar Pengantar Aplikasi Komputer, Yogyakarta: Deepublish, 2018.