SKRIPSI

PEMANFAATAN VPN (*VIRTUAL PRIVATE NETWORK*) SEBAGAI MEDIA PENGONTROL JARAK JAUH JARINGAN *MIKROTIK* UNTUK MENGAKSES SISTEM *SERVER* DAN MANAJEMEN *USER*

RYAN REYNALDY
D0217517

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS SULAWESI BARAT
MAJENE
2024

ABSTRAK

Perkembangan *internet* telah menjadi aspek penting dalam kehidupan, karena setiap orang dapat berkomunikasi dan bertukar informasi melalui *internet*. Pemerintah dan swasta memanfaatkan *internet* sebagai alat untuk memfasilitasi komunikasi dan pertukaran informasi. Informasi dapat dibagikan dengan cepat dan mudah, namun terdapat potensi resiko bocornya informasi sensitif. *Internet* merupakan salah satu media komunikasi yang mempunyai dampak positif dan negatif, seperti kecepatan dan keamanan. Untuk mengatasi masalah komunikasi data melalui jaringan publik, digunakan *Virtual Private Network* (VPN). VPN adalah koneksi *virtual* pribadi yang tidak dapat diakses secara fisik tetapi hanya *virtual*, yang memungkinkan pengguna mengakses dan berbagi informasi. *Transfer* data dari jaringan kompleks ke jaringan publik melibatkan *server* dan *client*, dengan banyak sistem operasi memiliki koneksi manual dan tidak ada jaringan *virtual* pribadi. Untuk mengatasi masalah ini, jaringan *virtual* pribadi harus dibuat sebagai *server* dan klien, yang memungkinkan *transfer* data dengan mudah. Hal ini dapat dicapai melalui paket *Mikrotik Virtual Private Network* (VPN).

Kata Kunci : VPN, Jaringan, *Internet*

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Pesatnya perkembangan *internet* saat ini telah dijadikan sebagai aspek penting dalam kehidupan. Setiap orang dapat berkomunikasi dan bertukar informasi satu sama lain melalui *internet*. Bahkan saat ini, sektor swasta dan pemerintah menggunakan *internet* sebagai bagian dari jaringan mereka untuk memfasilitasi pertukaran dan pertukaran informasi. Informasi dapat dikirim atau diterima dengan cepat dan mudah. Memang betul bahwa informasi bisa dikomunikasikan cara mudah, namun terdapat potensi kebocoran informasi pada tangan orang yang tidak bertanggung jawab. Hal ini karena sebagian besar kegiatan pertukaran informasi masih dilakukan melalui jaringan publik, sehingga pihak lain yang dianggap tidak berkepentingan dapat masuk dan mendapatkan informasi. *Internet* merupakan media komunikasi yang saat ini digunakan dimana-mana. Penggunaan *internet* memiliki banyak efek positif dan efek negatifnya seperti berbagai kejahatan seperti pencurian data.

Teknologi *internet* pernah digunakan oleh instansi-instansi maupun pada masyarakat umum sebagai jaringan komunikasi terbuka di mana pengguna dapat mengakses, berbagi, dan menambahkan informasi semudah mungkin, dan ada risiko tinggi hilangnya informasi rahasia yang akan merugikan. Masalah pada keamanan, penggunaan dengan mudah serta kecepatan transmisi (*transfer file*) merupakan aspek yang sangat penting padakomunikasi jaringan.

Untuk mengatasi masalah keamanan setiap komunikasi data yang dilakukan melalui *public network* (jaringan publik) maka diperlukan suatu *Virtual Private Network* (VPN). VPN (*Virtual Private Network*) adalah sebuah koneksi *Virtual* yang bersifat *Private* karena pada dasarnya jaringan ini tidak terdapat secara fisik namun hanya berupa jaringan secara *Virtual*, yang tidak semua orang mampu mengaksesnya. VPN (*Virtual Private Network*) dipergunakan buat melakukan transmisi paket data, yang terenkripsi sehingga tak praktis disadap oleh pihak yang tidak berwenang.

Aktivitas *transfer* data dari suatu kompleks perumahan di sekitar wilayah kompleks perumahan penduduk dalam hal ini diambil satu sampel yaitu operator suatu kompleks perumahan dan seluruh warga dalam hal ini pengguna jaringan *wifi*. Kebanyakan dalam pengolaan operasional suatu jaringan *mikrotik* pada suatu usaha masih bersifat manual dan belum memiliki lalu lintas jaringan *virtual* pribadi sehingga ditemukan kendala-kendala dalam menyelesaikan suatu pekerjaaan apabila dikerjakan dalam jarak jauh, sehingga aktivitas pekerjaan menjadi kurang efektif dan efisien.

Karena itu perlu dibangun sebuah jaringan *Virtual* yang bersifat pribadi sebagai *Server* di sekitar wilayah kompleks perumahan sebagai *Client*, sehingga bisa mempermudah untuk mengatasi permasalahan tersebut diperlukan suatu perancangan Jaringan *Virtual Private Network* (VPN) berbasis *Mikrotik*. Jaringan *Virtual Private Network* (VPN) berbasis *Mikrotik* merupakan jaringan transmisi paket data yang terenkripsi sehingga tak praktis disadap oleh pihak yang tidak berwenang.

Berdasarkan penjelasan di atas maka penulis berkeinginan untuk membangun suatu rancangan dengan mengangkat judul "**Pemanfaatan VPN (*Virtual Private Network)* Sebagai Media Pengontrol Jarak Jauh Jaringan *Mikrotik* Untuk Mengakses Sistem *Server* Dan Manajemen *User*".**

B. Rumusan Masalah

Berdasarkan uraian latar belakang masalah tersebut diatas, maka dapat dirumuskan penelitian yang dilakukan adalah:

1. Bagaimana merancang pemanfaatan VPN sebagai media pengontrol jarak jauh jaringan *Mikrotik* ?
2. Bagaimana merancang jaringan yang dapat melakukan *control* jarak jauh secara mudah dan prkatis?

C. Batasan Masalah

Pembahasan proposal penelitian ini tidak terlalu luas dan mudah dipahami maka penyusunan mambatasi ruang lingkup permasalahan pada :

1. Implementasi dirancang menggunakan *Mikrotik RB750*
2. Pemanfaatan VPN sebagai kontrol jarak jauh *mikrotik*

D. Tujuan dan Manfaat

1. Tujuan

a. Membangun jaringan bersifat *private* dengan menggunakan jaringan *public* yaitu *internet*.

b. Memudahkan bagi *admin* jaringan dalam mengakses dan mengkonfigurasi *mikrotik* dan *server* pada jaringan.

2. Manfaat

a. Menerapkan hasil belajar yang didapatkan selama di Program Studi S1 Teknik Informatika yang mengacu pada penerapan membangun sebuah jaringan sesuai dengan kebutuhannya pada lingkungan kampus Setelah melaksanakan kegiatan penelitian diharapkan penulis memiliki pengetahuan serta pengalaman yang lebih luas.

b. Mengetahui tentang konsep penerapan teknologi VPN sebagai media pengontrol jarak jauh jaringan *mikrotik* untuk mengakses *server* dan manajemen *user*.

BAB II

KAJIAN PUSTAKA

A. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas sebuah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Komputer dapat berhubungan satu dengan yang lainnya secara tidak terbatas baik dengan menggunakan kabel tembaga, *fiber* optik, *infrared*, gelombang *microwave,* bahkan bisa juga menggunakan satellite. Sebuah jaringan biasanya terdiri dari dua atau lebih PC yang saling berhubungan satu sama lain, dan berbagi sumber daya misalnya, CDROM, *printer*, pertukaran data, atau memungkinkan untuk berkomunikasi dengan lain secara elektronik. Komputer yang tersambung mungkin terkait dengan media tautan, saluran telepon, gelombang radio, satelit atau inframerah.

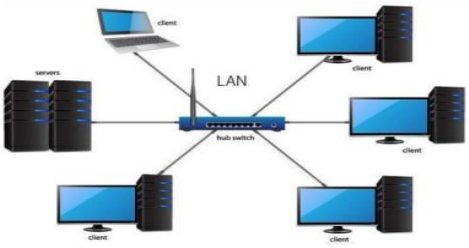
Jaringan komputer adalah kerangka kerja yang terdiri dari setidaknya dua komputer yang dihubungkan satu sama lain melalui media transmisi danmedia komunikasi sehingga mereka dapat berbagi informasi aplikasi dan menawarkan peralatanPC (Haryanto & Riadi, 2019).

Gambar 2.1 Jaringan Komputer

Sumber : (http://repository.upbatam.ac.id/)

1.LAN *(Local Area Network)*

Jaringan yang terdapat didalam gedung atau kampus yang berjarak sampai dengan beberapa kilometer. LAN sering digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam instansiatau perusahaan untuk dan saling bertukar informasi.



Gambar 2.2 Jaringan LAN

Sumber : (http://repository.upbatam.ac.id/)

2. MAN *(Metropolitan Area Network)*

Jaringan versi LAN yang berukuran lebih besar, menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup instansi –instansi perusahaan

yang letaknya berdekatan atau antar sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi atau umum. MAN juga menunjang data dan suara bahkan dapat digunakan untuk aplikasi TV kabel.

Gambar 2.3 Jaringan MAN

Sumber : (http://repository.upbatam.ac.id/)

3. WAN *(Wide Area Network)*

Jangkauan jaringannya mencakup daerah geografis yang luas seringkali mencakup negara bahkan benua. Teknologi yang digunakan hampir sama dengan LAN.

Gambar 2.4 Jaringan WAN

Sumber : (http://repository.upbatam.ac.id/)

B. *Virtual Private Network*

Virtual Private Network (VPN) adalah sebuah jaringan *private* yang dibuat di atas jaringan *public* dengan menggunakan *internet* sebagai media komunikasinya. (Stalling 2003).

Menurut Efendi (2010), karena infrastruktur VPN menggunakan infrastruktur telekomunikasi umum, maka dalam VPN harus menyediakan beberapa komponen, antara lain :

1. Konfigurasi, harus mendukung skalabilitas platform yang digunakan, mulai dari konfigurasi untuk instansikecil sampai tingkat enterprise (perusahaan besar).
2. Keamanan, antara lain dengan tunneling (pembungkusan paket data), enkripsi, autentikasi paket, autentikasi pemakai dan kontrol akses
3. Layanan-layanan VPN, antara lain fungsi *Quality of Services (QoS)*, layanan routing VPN yang menggunakan protocol routing seperti BGP, OSPF dan EIGRP.
4. Peralatan, antara lain *Firewall*, pendeteksi pengganggu, dan auditing keamanan manajemen, untuk memonitor jaringan VPN.

Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut tunneling. Berikut adalah beberapa kriteria yang harus dipenuhi oleh VPN:

1. *User Authentication*: VPN harus mampu mengklarifikasi identitas klien serta membatasi hak akses *user* sesuai dengan otoritasnya. VPN juga dituntut mampu memantau aktifitas klien tentang masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis resource yang diakses oleh klien tersebut. Address Management VPN harus dapat mencantumkan alamat klien pada intranet dan memastikan alamat tersebut tetap rahasia.
2. *Data Encryption*: Data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak atau klien yang tidak berwenang.
3. *Key Management*: VPN harus mampu membuat dan memperbarui encryption key untuk *server* dan *client*.
4. *Multiprotocol Support*: VPN harus mampu menangani berbagai macam protocol dalam jaringan publik seperti IP, IPX , dan sebagainya. Terdapat tiga protokol yang hingga saat ini paling banyak digunakan untuk VPN. Ketiga protokol tersebut antara lain adalah *Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPSec SOCKS CIPE*

Protokol-protokol di atas menekankan pada authentikasi dan enkripsi dalam VPN. Adanya sistem otentifikasi akan mengijinkan *client* dan *server* untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat melewati jaringan publik. Intranet merupakan koneksi VPN yang membuka jalur komunikasi

pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan publik seperti *internet*. (Efendi, 2010).

Menurut Harmening (2013) jaringan personal buatan yang bias dikenal dengan *virtual privatee network* dan biasanya disingkat VPN adalah jaringan personal yang dibangun seolah-olah berada dalam jaringan umum yang dapat digunakan sebagai media komunikasi data dan informasi yang aman. Menurut (Muhsyi, 2019) VPN (*Virtual Private Network*) adalah variasi jaringan komputer yang tingkatnya lebih advanced dibandingkan jaringan komputer biasa. Dengan demikian tersebut maka akan didapatkan hak dan pengaturan yang samaseperti halnya berada didalam LAN itu sendiri, meskipun sebelumnya menggunakan jaringan *public*. *VirtualPrivate Network* (VPN) merupakan salah satu alternatif untuk pengamanan data karena bersifat privat". VPN memungkinkan pengguna dapat masuk ke dalam jaringan lokal, memungkinkan pengguna untuk mengambil data dari dalam jaringan lokal serta melakukan remote pada perangkat yang ada dijaringan tersebut (Farly K et all 2017)".

Dari cara pandang jaringan, salah satu masalah jaringan *internet* (IP *Public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Sedangkan dari cara pandang perusahaan. IP adalah kebutuhan dasar untuk melakukan pertukaran data antara instansi cabangatau dengan rekanan perusahaan. *Virtual Private Network* (VPN) muncul untuk mengatasi persoalan tersebut. Sebuahjaringan perusahaan yang menggunakan infrastruktur IP untuk berhubungan dengan instansi cabangnya dengan

cara pengaamanan secara *private* dengan melakukan pengamanan terhadap jenis-jenis VPN.

C. PPTP

Point-to-Point Tunneling Protocol (PPTP) merupakan teknologi baru pada jaringan yang mendukung multi protocol *Virtual Private Networks* (VPN) sehingga memungkinkan pengguna untuk mengakses jaringan suatu organisasi secara lebih aman melalui *internet*. Dengan menggunakan PPTP, pengguna jarak jauh dapat memanfaatkan *Microsoft Windows NT Workstation, Windows 95*, dan sistem yang mendukung *PPP* lainnya untuk melakukan dial up ke *ISP* lokal untuk terhubung secara lebih aman ke dalam jaringan lokal suatu organisasi dengan menggunakan *internet*.

PPTP memungkinkan koneksi yang aman dan terpercaya kepada jaringan organisasi melalui *internet*. Hal ini sangat berguna untuk anggota organisasi yang bepergian dan harus mengakses jaringan organisasinya dari jarak jauh, untuk mengecek email, atau untuk melakukan aktifitas lainnya. Dengan *PPTP*, seorang pengguna dapat menghubungi nomor telepon lokal dengan menggunakan modem analog maupun modem *ISDN* untuk mengakses *ISP* dan kemudian masuk ke dalam jaringan organisasi. Setiap sesi koneksi *PPTP* dapat membuat koneksi yang aman dari *internet* ke pemakai dan kembali menuju ke jaringan organisasi. Koneksi secara lokal dari pemakai ke ISP akan menghubungkannya ke dalam *hardware device Front-End Processor (FEP*) yang dapat berada dalam kota yang sama dengan

pemakai. FEP kemudian menghubungkan diri dengan NT *Server* yang berada di kota yang berbeda melalui WAN seperti *Frame Relay atau X.25.* FEP melakukan hal ini dengan mengambil paket PPP dari pemakai dan melakukan tunneling melalui WAN. Dikarena PPTP mendukung banyak protokol *(IP, IPX dan NetBEUI)* maka PPTP dapat digunakan untuk mengakses berbagai macam infrastruktur LAN. PPTP juga mudah dan murah untuk diimplementasikan. Banyak organisasi yang dapat menggunakan PPTP ini untuk menyediakan koneksi yang murah, mudah dan aman ke dalam jaringan. Hal yang terpenting dengan menggunakan PPTP adalah konfigurasi jaringan organisasi tidak perlu berubah, termasuk pengalamatan komputer-komputer di dalam jaringan intranet. WAN *virtual* mendukung penggunaan PPTP melalui *backbone IP* dan sangat efektif untuk digunakan.

1. Entitas Yang Terlibat Dalam PPTP

Untuk membangun PPTP pada umumnya dibutuhkan tiga entitas, antara lain: *PPTP client, Network Access Server (NAS),* dan PPTP *server*. Akan tetapi tidak diperlukan NAS dalam membuat PPTP tunnel saat menggunakan PPTP *client* yang terhubung dengan PPTP *server* pada LAN yang sama.

a. PPTP *Client*

Sebuah komputer yang mendukung protokol jaringan PPTP, misalnya *Microsoft Client,* dapat melakukan koneksi ke *server* PPTP dengan dua cara:

a) Menggunakan NAS-ISP yang mendukung koneksi PPP
b) Menggunakan sambungan LAN dengan TCP/IP diaktifkan untuk terhubung ke *server* PPTP. PPTP *client* yang menggunakan NAS-ISP

harus dikonfigurasi dengan modem dan perangkat VPN untuk membuat sambungan terpisah ke ISP dan *server* PPTP. Sambungan yang pertama adalah sambungan dial-up menggunakan protokol PPP melalui modem ke salah satu penyedia layanan *internet*. Yang kedua adalah sambungan koneksi VPN menggunakan PPTP dengan melalui modem dan koneksi ISP, ke tunnel di *internet* lalu ke perangkat VPN pada *server* PPTP. Sambungan yang kedua memerlukan sambungan pertama karena tunnel antara perangkat VPN dibangun dengan menggunakan modem dan koneksi PPP ke *internet*. Pengecualian untuk kedua persyaratan sambungan ini, yaitu menggunakan PPTP untuk membuat VPN di antara komputer-komputer yang secara fisik terhubung ke jaringan LAN perusahaan *private*. Dalam skenario ini, PPTP *client* sudah terhubung ke jaringan dan hanya menggunakan Dial-Up *Network*ing dengan perangkat VPN untuk membuat sambungan ke *server* PPTP pada LAN. Paket PPTP dari PPTP *client* secara remote access dan PPTP *client* pada LAN lokal akan diproses dengan cara yang berbeda. Paket PPTP dari PPTP *client* secara remote access akan ditempatkan pada media fisik perangkat teletomunikasi, sementara PPTP paket dari PPTP *client* lokal LAN ditempatkan pada media fisik *network* adapter.

b. *Network Access Server (NAS)*

ISP menggunakan NAS untuk mendukung *client* yang melakukan dial dengan menggunakan protokol, seperti SLIP atau PPP untuk mendapatkan

akses ke *internet*. Namun, untuk mendukung *client* dengan PPTP aktif maka NAS harus menyediakan layanan PPP. *Server* akses jaringan ISP ini dirancang dan dibangun untuk mengakomodasi banyaknya jumlah *client* yang dial-in. NAS dibangun oleh perusahaanperusahaan seperti *3COM, Ascend, ECI Telematics,* dan *US Robotika* yang merupakan anggota dari Forum PPTP.

2. PPTP *Server*

PPTP *server* adalah *server* dengan kemampuan routing yang terhubung ke jaringan *private* dan ke *internet*. Sebuah PPTP *server* dapat ditentukan sebagai komputer yang menjalankan *Windows NT Server versi 4.0* dan Remote *Access Service (RAS*). PPTP diinstal sebagai protokol jaringan. Selama instalasi, PPTP dikonfigurasi dengan menambahkan perangkat *virtual* yang disebut sebagai *VPN ke RAS dan Dial-Up Networking*.

3. Arsitektur PPTP

Dalam Afrianto dan Setiawan (2015) disebutkan bahwa tunneling PPTP memiliki beberapa arsitektur didalam pembentukannya, yaitu terdiri dari:

a. PPTP *Connection and Communication*

PPP adalah remote access protocol yang digunakan oleh PPTP untuk mengirim data multi protokol melintasi jaringan berbasis TCP/IP. PPP mengenkapsulasi paket IP, IPX, dan NetBEUI di antara frame PPP dan mengirimkan paket terenkapsulasi tersebut dengan menciptakan suatu link point to-point antara komputer pengirim dan penerima. Sesi PPTP dimulai

oleh *client* yang melakukan dial up NAS-ISP. Protokol PPP yang digunakan untuk membuat sambungan dial-up antara *client* dengan *server* akses jaringan melakukan tiga fungsi sebagai berikut :

a) Membangun dan mengakhiri sambungan fisik , PPP protokol menggunakan rangkaian yang ditetapkan dalam RFC 1661 untuk membangun dan memelihara hubungan antara remote *computer*.

b) Melakukan authentikasi, pengguna PPTP diauthentikasi oleh *client* dengan menggunakan protokol PPP.

c) Menciptakan PPP datagram, Datagram ini dienkripsi IPX, NetBEUI, atau paket-paket TCP/IP. PPP membuat datagram yang berisi satu atau lebih paket data TCP/IP, IPX, atau NetBEUI terenkripsi. Karena paket-paket jaringan dienkripsi, maka semua lalu lintas antara *client* PPP dan NAS akan menjadi aman. Dalam beberapa situasi, remote *client* dapat memiliki akses langsung ke jaringan TCP/IP, seperti halnya *internet*. Sebagai contoh, sebuah laptop dengan kartu jaringan dapat menggunakan *internet* di ruang pertemuan. Dengan sambungan IP langsung, koneksi awal PPP ke sebuah ISP menjadi tidak perlu. *Client* dapat melakukan koneksi ke *server* PPTP, tanpa terlebih dahulu melakukan koneksi PPP ke ISP.

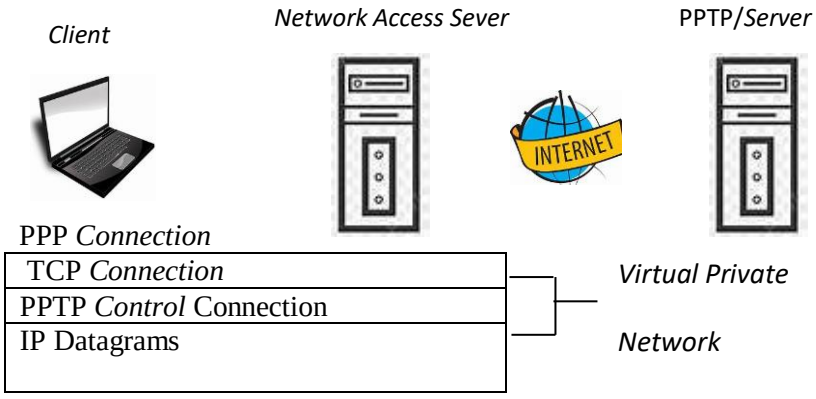
b. PPTP *Control Connection*

Protokol PPTP menentukan rangkaian pesan kontrol yang dikirim antara PPTP-*enabled client* dan PPTP *server*. Pesan-pesan *control* membangun, memelihara dan mengakhiri PPTP tunnel. Pesan-pesan kontrol dikirim dalam

paket-paket *control* dalam datagram TCP. Satu koneksi TCP dibuat antara *client* PPTP dan *server* PPTP. Sambungan ini digunakan untuk mengendalikan pertukaran pesan.

c. PPTP Data Transmission

Setelah PPTP tunnel dibuat, data pengguna dikirim antara PPTP *client* dan PPTP *server*. Data yang dikirimkan dalam IP datagram berisi paket PPP. IP datagram dibuat menggunakan versi modifikasi dari protokol *Internet Generic Routing Encapsulation* (GRE). IP header pengirim menyediakan informasi yang diperlukan bagi datagram untuk melintasi *internet*. GRE *header* digunakan untuk mengenkapsulasi paket PPP yang ada di dalam IP datagram. Paket PPP telah dibuat oleh RAS.



Gambar 2.5 Arsitektur PPTP

Sumber : (http://repository.upbatam.ac.id/)

4. Keamanan PPTP

PPTP memperluas autentikasi dan enkripsi yang tersedia untuk keamanan komputer yang menjalankan RAS pada Windows NT *Server* versi 4.0 dan *Windows NT Workstation* versi 4.0 menjadi *client* PPTP di *internet*. PPTP juga dapat melindungi PPTP *server* dan jaringan *private*. Meskipun memiliki keamanan yang ketat, sangat sederhana untuk menggunakan PPTP dengan *firewall* yang ada (Mufida 2017). Keamanan yang tersedia pada PPTP adalah sebagai berikut:

a. Autentikasi

Authentikasi saat awal dial-in mungkin diperlukan oleh sebuah ISP *network access server*. Jika authentikasi ini dibutuhkan, maka untuk *login* ke ISP *network access server* akan menjadi lebih ketat, namun hal itu tidak berkaitan dengan authentikasi berbasis Windows NT. Setiap *client* menerapkan persyaratan untuk ISP mereka sebagai Dial-Up *Networking entry* untuk ISP tersebut. Di sisi lain, jika Windows NT *Server* versi 4.0 dikonfigurasi sebagai PPTP *server*, ia mengontrol semua akses ke jaringan *private client*. Yakni, PPTP *server* merupakan pintu gerbang ke jaringan *private client*. Semua *client* PPTP harus memberikan nama pengguna dan *password*. Karena itu, remote access logon menggunakan komputer yang berjalan pada *Windows NT Server versi 4.0* atau *Windows NT Workstation versi 4.0* memiliki keamanan seperti logon dari Windows NT berbasis komputer yang terhubung ke LAN lokal. Authentikasi dari remote PPTP

client dilakukan dengan menggunakan metode authentikasi PPP yang sama dengan yang digunakan untuk panggilan langsung *client* RAS ke *server* RAS. Implementasi *Microsoft* dari *Remote Access Service* (RAS) mendukung skema authentikasi *Challenge Handshake Authentication Protocol* (CHAP), *Microsoft Challenge Handshake Authentication Protocol* (MSCHAP), dan *Password Authentication Protocol* (PAP). Akun pengguna dari *remote user* berada pada layanan direktori *Windows* NT *Server* versi 4.0 dan diatur melalui Manager Pengguna untuk domain. Hal ini menyediakan sentralisasi administrasi yang terintegrasi dengan jaringan *private* tempat akun pengguna. Hanya akun yang telah diberikan akses khusus ke jaringan melalui domain terpercaya yang akan diijinkan masuk. Pengelolaan akun pengguna secara hati-hati diperlukan untuk mengurangi risiko keamanan.

b. Kontrol Akses

Setelah melakukan authentikasi, seluruh akses ke LAN *private* menggunakan Windows NT yang telah ada berdasarkan struktur keamanannya. Akses terhadap resource pada drive NTFS atau terhadap resource jaringan memerlukan perizinan, seolah-olah telah terkoneksi secara langsung ke LAN.

c. Enkripsi Data

Untuk enkripsi data, PPTP menggunakan RAS untuk proses enkripsi sharedsecret. Hal ini merujuk pada shared-secret karena kedua end point pada koneksi membagi kunci enkripsi. Pada implementasi Microsofts RAS,

rahasia yang dibagi adalah *password* pengguna. PPTP menggunakan enkripsi PPP dan skema kompresi PPP. *Compression Control Protocol* (CCP) digunakan untuk menegosiasi enkripsi yang digunakan.

Username dan *password* tersedia untuk *server* dan disediakan oleh *client.* Kunci enkripsi dibangkitkan menggunakan hash terhadap *password* yang tersimpan pada *client* dan *server*. Standard RSA RC4 digunakan untuk membuat enkripsi data dengan 40- bit *session* key berdasarkan pada *password client* Lalu, kunci ini digunakan untuk mengenkripsi dan dekripsi seluruh data yang telah ditukar antara PPTP *client* dan *server*. Data pada paket PPP telah dienkripsi. Paket PPP berisi blok data terenkripsi yang kemudian diisi ke dalam IP datagram untuk routing

d. PPTP *Packet Filtering*

Keamanan jaringan dari penyusup dapat ditingkatkan dengan melakukan PPTP filtering pada PPTP *server*. Ketika PPTP filtering telah diaktifkan, PPTP *server* pada jaringan menyetujui dan hanya mengirimkan paket PPTP saja. Hal ini mencegah seluruh tipe paket yang lain yang masuk ke dalam jaringan. Lalu lintas PPTP menggunakan port 1723.

D. *Router Mikrotik*

Juilek dan Zalud (2012) *Mikrotik* adalah sistem operasi unix yang dikembangkan secara komersial dan dirancang khusu sebagai sistem operasi yang

focus kepada perangkat *network* sebagai perangkat komponen aktif seperti *router, acces point, switch router* dan banyak lagi. *Router* befungsi untuk menghubungkan dari satu jaringan ke jaringan yang lain. Penerapan *Router* berada pada lapisan *Network* di model OSI. *Router* dianggap memiliki kemampuan Routing, dalam arti *router* dapat mengetahui kemana rute perjalanan (Packet) akan dilewatkan (Sofana Iwan, 2017). Simbol khusus untuk menandakan sebuah perangkat *Router* digambarkan seperti dibawah ini.

Gambar 2.6 Simbol *Router*

Sumber : (http://repository.upbatam.ac.id/)

1. Sejarah *Mikrotik*

Mikrotik dibangun pada tahun 1995 oleh Jhon Trully dan Arnis Riesktinis, sampai saat ini berbagai perangkat *mikrotik* telah tersebar penjualan nya diseluruh dunia. Perusahaan *mikrotik* mengembangkan sebuah sistem operasi *Router* yang berfitur lengkap yang disebut *Router*OS. Tahap perkembangan *mikrotik* selanjutnya pada tahun 2002, yaitu perusahaan *mikrotik* memproduksi perangkat keras dengan merek *Router*Board. Dari berjalan nya waktu, *Router*BOARD mengembangkan desain dan fitur baru untuk membantu perusahaan kecil, penyedia jasa layanan *internet*, dan penyedia jasa layanan nirkabel untuk mengembangkan usaha nya.

2. *Mikrotik Router*OS

*Mikrotik Router*OS merupakan suatu sistem operasi yang diperuntukkan sebagai *network router*. *Mikrotik Router*OS sendiri adalah sistem operasi dan perangkat lunak yang dapat membuat komputer biasa menjadi sebuah *router network* yang andal dan memiliki banyak fitur menarik (Sofana Iwan, 2017).

3. *Mikrotik* Licence

Mikrotik Licence menerapkan sebuah sistem operasi berlisensi. Untuk dapat menggunakan seluruh fitur hebat secara penuh yang diuraikan dari fitur level 0 hingga level 6 sampai saat ini, harus membeli lisensi yang akan digunakan satu lisensi hanya valid untuk satu buah harddisk.

4. *Mikrotik Router BOARD*

Sebagian besar orang menyebut *Mikrotik Router* sebagai *RouterBOARD. Mikrotik Router* dibagi 2 kelompok, yaitu:

a. Integrated yaitu sebuah perangkat *router* lengkap dengan casing dan power supply. Contoh nya RB750, RB751U-2HnD.

Gambar 2.7 *Mikrotik RB750*

Sumber : (http://repository.upbatam.ac.id/)

b. *RouterBOARD* yaitu sebuah motherboard tidak memiliki power supply, interface, dan casing. Jenis *router* seperti ini dapat di kostum untuk disesuaikan dengan kebutuhan penggunaan nya. Contoh nya RB411 dan RB800.

Gambar 2.8 *Mikrotik* RB800

Sumber : (http://repository.upbatam.ac.id/)

E. Penelitian Terdahulu

Penelitian terdahulu merupakan sebagai acuan peneliti dalam melakukan penelitian ini. Keterkaitan dengan judul, metode, dan masalah penelitian yang berhubungan oleh penelian ini dengan topik Pemanfaatan VPN Sebagai Media Pengotrol jarak jauh jaringan *Mikrotik.*

Tabel 2.1 Penelitian Terdahulu

No	Nama dan Tahun Penelitian	Judul Penelitian	Hasil Penelitian	Perbedaan dan Persamaan Penelitian
1	Rino Subekti (2020)	Implementasi *Virtual Private Network* (Vpn) Sebagai Solusi	Pada penelitian ini penulis menggunakan protokol	Penelitian sebelumnya menerapkan penggunaan protokol *EoIP Tunel*,dengan

		Security Selama *Work From Home*	*EoIP Tunel*, perusahaan yang sudah mempunyai koneksi *internet*, selain mendapatkan *bandwidth internet*, dapat juga memanfaatkan jaringan publik atau *internet*nya sebagai penghubung jalur *private* atau biasa dikenal dengan intranet.	koneksi *internet*, namun pada peneltian ini memanfaatkan jaringan *public* sebagai jalur penghubung *private.*
2	Ayu Purnama Sari (2020)	Perancangan Jaringan *Virtual Private Network* Berbasis *Ip Security* Menggunakan *Router Mikrotik*	Pada penelitian ini penulis menggunakan *VPN IPsec* menjadikan jalur komunikasi data yang aman. Dan dapat diakses dari jaringan publik seperti, *wifi* dan *hotspot.* Ini dikarenakan *Tunneling* dari *VPN* yang memberikan jalur khusus untuk masuk ke jaringan lokal. Dan ditambah	Penelitian sebelumnya menerapkan penggunaan jaringan *VPN*, namun penelitian ini menggunakan*IPsecurity* yang dapat membuat jaringan *VPN berbasis Ip Security* menjadi lebih aman menggunakan *Router Mikrotik*

			keamanan *data* dengan *protocol Ipsec*	
3	Petrus Anton Bagyono (2021)	Implementasi Vpn Untuk Akses *Server* Melalui Perangkat Mobile Pada Jaringan Komputer Smk Triatma Jaya Semarang	Pada penelitian ini penulis menggunakan VPN yang dapat membangun koneksi pada jaringan *public* (*internet*) sebagai sarana pengaksesan file serta kontrol jarak jauh (remote) *dan* pada *server* secara cepat, praktis, dan dari mana saja melalui perangkat mobile berbasis *Android*	Penelitian sebelumnya menerapkan penggunaan jaringan *VPN* sebagai kontrol jarak jauh (remote) pada *server*melalui perangkat mobile berbasis *Android*
4	Hendra Supendar (2016)	Implementasi Remote Site Pada *Virtual Private Network* Berbasis *Mikrotik*	Pada penelitian ini penulis menggunakan VPN dapat mempermudah dan efeisiensi waktu dalam pertukaran data hanya dengan mengaktifkan VPN *client*	Penelitian sebelumnya menerapkan penggunaan melakukan *sniffing* pada jaringan VPN di CMS. dan hasilnya adalah pada koneksi dengan VPN terdapat kompres data pada IP Publik dan enkapsulasi pada IP lokal.
5	Lia Umaroh (2020)	Implementasi *Virtual Private*	Pada penelitian ini penulis	Penelitian sebelumnya menerapkan

		Network (Vpn) Di Perpustakaan Universitas Islam Malang	menggunakan VPN di Perpustakaan UNISMA selain untuk mempermudah dan mempercepat koneksi *internet* juga digunakan untuk melindungi privasi data.	penggunaan VPN dengan *server mikrotik router operating system*. *Mikrotik* tersebut digunakan untuk menjadikan komputer menjadi *router network* yang memiliki berbagai fitur untuk *IP network* dan jaringan *wireless*, serta digunakan untuk *ISP* dan *provider hotspot*
6	Sepriwan (2019)	Pemanfaatan VPN Sebagai Media Pengotrol jarak jauh *Hotspot* Berbayar serta penggunaan aplikasi *Mikhmon* sebagai *Voucher Generate* dan manajemen *user*	Hasil penelitian ini menunjukkan alat yang dibuat dapat berfungsi dengan baik dan dikembangkan untuk skala yang lebih besar.	Penelitian sebelumnya penggunaan VPN sebagai pengontrol jarak jauh dengan *user mikrotik* sebagai pengendali proses, dengan pengontrolan *hotspot* berbayar menggunakan aplikasi *Mikhmon* sebagai voucher generate dn manajemen *user mikrotik*
7	Darma Putra Hadinata (2014)	Perancangan dan Implementasi VPN *Server* sebagai media *control* jarak jauh sistem pemantau jaringan *The Dude* di PT. Lintas data prima	DenganVPN memberikan solusi keamanan jaringan dalam proses pertukaran data karena menggunakan jalur *private* yang terenkripsi. teknologi VPN, *client* dapat melakukan kontrol jarak	Penelitian sebelumnya penggunaan VPN sebagai pengontrol jaringan, dengan teknologi VPN, pengontrol jarak jauh hingga *client* dapat melakukan kontrol jarak jauh aplikasi monitoring jaringan the dude

			jauh aplikasi monitoring jaringan *the dude* darimana saja jika terhubung dengan *internet*.	

BAB III

METODE PENELITIAN

A. Metode Penelitian

Tipe penelitian yang dipakai adalah tipe penelitian terapan, dan dideskripsikan di dalam penelitian ini adalah penelitian rancang bangun jaringan VPN dengan menggunakan *Router Mikrotik*. Tahapan ini berisi tahapan yang dilakukan dalam proses penelitian termasuk di dalamnnya menjelaskan bagaimana penertapan metode pengembangan sistem atau metode komputasi pada penelitian yang sedang dilakukan.

Jenis penelitian yang digunakan dalam penyusunan proposal penelitianini dalam hal pengumpulan data dan informasi antara lain :

a. Secara Langsung

Secara langsung artinya di dalam memperoleh data-data yang dibutuhkan, maka diadakan wawancara langsung dengan yang berkaitan langsung dengan objek yang diteliti

b. Secara Tidak Langsung

Secara tidak langsung artinya berpedoman pada buku-buku yang berkaitan dan berhubungan langsung dengan materi yang dilaksanakan, seperti buku pemrograman tentang *Mikrotik.*

B. Tehnik Pengumpulan Data

Tehnik pengumpulan dilakukan untuk mengumpulkan dan mengoreksi data dari berbagai sumber, informasi atau data. Menggunakan metode observasi atau pengamatan langsung ke objek penelitian serta metode wawancara kepada pihak yang berkaitan dengan objek yang akan diteliti.

1. Moetode Observasi

Dengan melakukan pengamatan langsung pada objek yang diteliti. Dari hasil observasi peneliti dapat memperoleh data yang berhubungan dengan objek penelitian yang berguna dalam merancang dan membangun Jaringan *Virtual Private Network* (VPN) Berbasis *Mikrotik.*

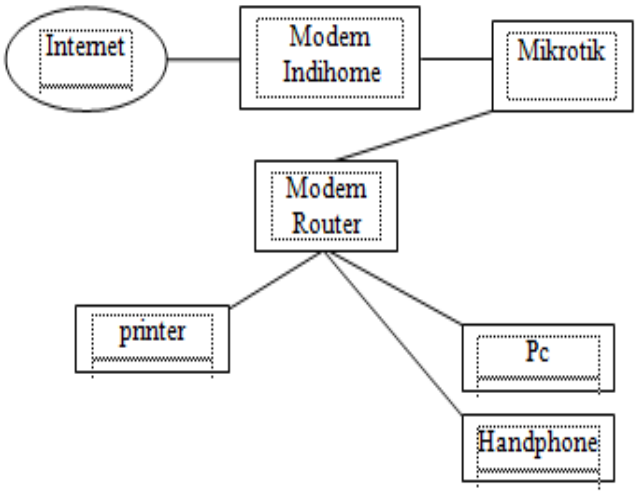
2.Metode Wawancara

Dalam pengambilan data pada objek yang akan diteliti akandilakukan wawancara kepada pihak yang berkaitan dengan objek yang akan diteliti, kendala apa saja yang didapatkan pada sistem yang berjalan saat ini,khususnya pada sistem jaringan *Virtual Private Network* berbasis *Mikrotik*.

C. Analisa Jaringan

Ditahap ini setelah peneliti menganalisa jaringan yang tersebut, peneliti lanjut ketahap rancangan jaringan yang akan dibangun. Sebelum menentukan rancangan jaringan VPN yang akan dibangun, peneliti membuat topologi jaringan yang untuk dibangun. Ditahap ini, peneliti menentukan posisi-posisi perangkat sesuai dengan topologi untuk akses jaringan *internet* menggunakan ip *publik* serta posisi perangkat-

perangkat yang berada dijaringan lokal melalui topologi jaringan yang dibuat Topologi yang digunakan pada penelitian ini bahwa Pemanfaatan VPN Sebagai Media Pengotrol jarak jauh jaringan *Mikrotik* yang sederhana dapat dilihat pada gambar berikut ini.



Gambar 3.1 Analisa Jaringan

Sumber : (Peneliti, 2024)

D. Tahapan Rencana Implementasi Jaringan

Pada tahap ini setelah peneliti menggambarkan topologi jaringan yang akan dibangun, tahapan selanjutnya akan diuraikan dibawah ini.

1. Menyesuaikan dan menghubungkan letak posisi perangkat sesuai dengan topologi yang dibuat. Penambahan *mikrotik* yang terhubung menggunakan kabel utp di Ethernet 1 modem ZTE akan dihubungkan kabel utp ke Ethernet 1 yang terdapat di*router mikrotik*.

2. Di ethernet 2 *mikrotik* akan dihubungkan kabel utp ke Ethernet laptop untuk sementara karena *mikrotik* akan dikonfigurasi oleh peneliti.

3. Di ethernet 3 *mikrotik* akan dihubungkan kabel utp ke Ethernet 1 tp-link wireless *router* dengan tujuan tp-link wirekewss *router* sebagai accses point pemancar *wifi* untuk perangkat-perangkat yang berada disekitarnya.

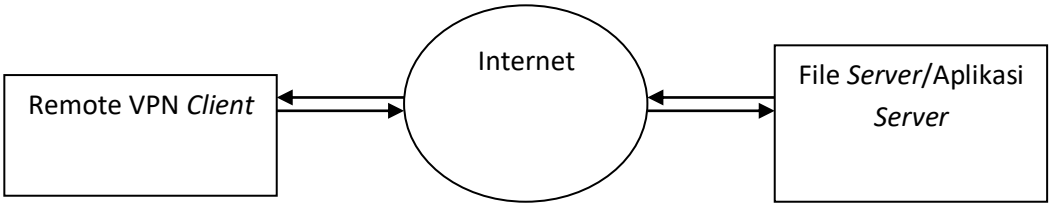
4. Peneliti akan mengonfigurasi *mikrotik* diantaranya setting *user login mikrotik* agar *mikrotik* nya aman dari pihak luar yang ingin melakukan *login* pada *mikrotik*, setting IP Publik pada *mikrotik* yang didapat dari ISP Astinet, setting pembagian alamat ip address pada jaringan lokal sesuai dengan topologi yang sudah dibuat peneliti.

5. Setelah konfigurasi jaringan wan dan lan pada *mikrotik* selesai, tahap selanjutnya peneliti akan mensetting konfigurasi jaringan vpn yang akan dibangun pada *mikrotik* beserta jenis tunnel vpn yang digunakan

6. Tahapan selanjutnya ketika konfigurasi sudah semestinya dilakukan, peneliti akan melakukan uji coba menggunakan fitur vpn tersebut dari luar area dengan remote to site ke *mikrotik* dan remote desktop ke komputer lokal yang berada area.

E. Rancangan Topologi

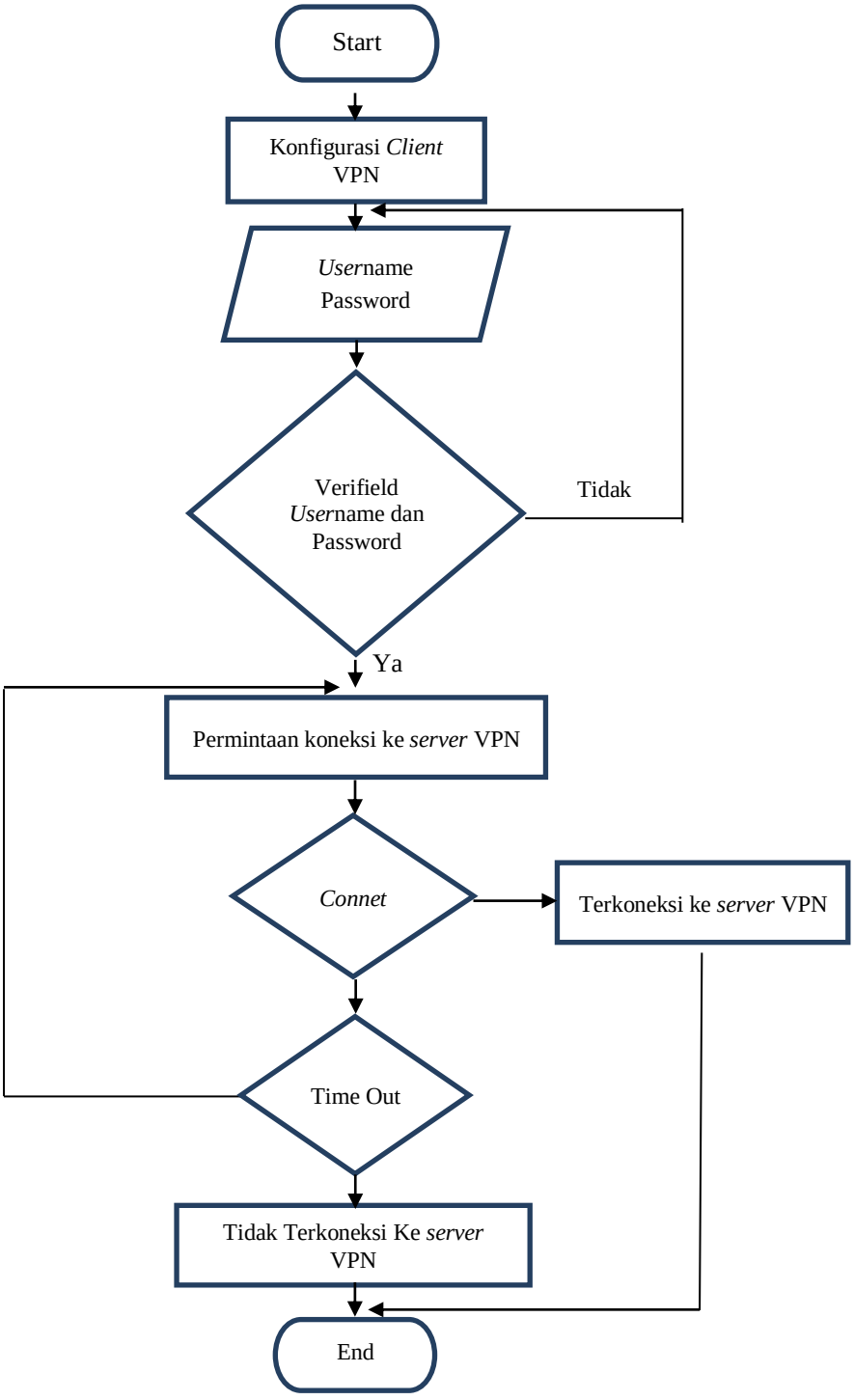
Topologi yang digunakan pada penelitian ini bahwa Pemanfaatan VPN Sebagai Media Pengotrol jarak jauh jaringan *Mikrotik* yang sederhana dapat dilihat pada gambar berikut ini.



Gambar 3.2 Topologi jaringan

Sumber : (Peneliti, 2024)

F. Flowchart VPN



Gambar 3.3 Flowchart VPN
Sumber : (Peneliti, 2024)

DAFTAR PUSTAKA

Afrianto, I. & Setiawan, E.B. 2015. Kajian *Virtual Private Network* (VPN) sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom). Majalah Ilmiah UNIKOM, 12(1), 43–52. https://doi.org/10.34010/miu.v12i1.34

Efendi (2010), Merancang jaringan Komunikasi VolP Sederhana dengna *Server* ColP Trixbox yang dilengkapi VQnajager dan Open VPN. Semarang.

Farly, K. A., Najoan, X. B. N., & Lumenta, A.S.M. 2017. Perancangan dan Implementasi VPN *Server* dengan Menggunakan Protokol SSTP (Secure Socket Tunneling Protocol): Studi Kasus Kampus Universitas Sam Ratulangi. Jurnal Teknik Informatika, 11(1). https://doi.org/10.35793/jti.11.1.2017.16745

Jílek, T., & Žalud, L. (2012). Security of remote management of embedded systems running *Mikrotik Router*OS operating system using proprietary protocols. IFAC Proceedings Volumes (IFAC-PapersOnline), 11(PART 1), 169–173. https://doi.org/10.3182/20120523-3-cz3015.00034

Haryanto,M.D.,&Riadi,I.(2019).AnalisaDanOptimalisasiJaringanMenggunakanTeknikLoad Balancing.Jurnal Sarjana teknik Informatika 2.

Jílek, T., & Žalud, L. (2012). Security of remote management of embedded systems running *Mikrotik Router*OS operating system using proprietary protocols. IFAC Proceedings Volumes (IFAC-PapersOnline), 11(PART 1), 169–173. https://doi.org/10.3182/20120523-3-cz3015.00034

Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site *Mikrotik* VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. Jurnal Matrik, 16(2), 9. https://doi.org/10.30812/matrik.v16i2.7

Muhsyi,A.(2019).MembangunJaringan*VirtualPrivateNetwork*(Vpn)DenganMetodeTunnelingMenggunakanUbuntu11.10PadaLaboratoriumJaringanSTMIKPPKIAPradnya….*JurnalTeknologiInformasi:Teori,Konsep,Dan…*,1–4.https://www.neliti.com/*public*ations/142018/membangun-jaringan-*virtual-private-network*-vpn-dengan-metode-tunneling-menggunak.

Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan *Virtual Private Network* IPSecurity*Router Mikrotik .JurnalPROSISKO, 7*(2),150–164.

Sofana Iwan, 2017). Jaringan Komputer Berbasis *Mikrotik*. In Jaringan *computer*.

Stalling.W.” Data and *Computer* Communications, Macmillan Publishing Company”, 2003.

Welcome to UPB Repository. UPB Repository. (n.d.-a). http://repository.upbatam.ac.id/