Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP

Implementation of L2TP / IPSec Protocol and Port Forwarding for Remote Mikrotik on Dynamic IP Networks

Hedy Pratama[*1], Nila Feby Puspitasari[2]
[1] Informatika, Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
[2] Teknik Informatika, Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
E-mail: ***[1]hedipras@gmail.com,** **[2]nilafeby@amikom.ac.id**

Abstrak

Salah satu cara yang dilakukan untuk menjaga dan meningkatkan kualitas layanan yang diberikan oleh suatu Perusahaan XYZ, seorang administrator setiap saat memonitoring lalu lintas data dengan mengakses router dan access point untuk mengetahui kondisi jaringan. Hal tersebut hanya dapat dilakukan Administrator ketika sedang berada dalam jaringan lokal. Permasalahannya, ketika Administrator berada pada jaringan publik, maka tidak dapat mengakses router dan perangkat access point yang ada. Hal ini dikarenakan IP publik yang didapatkan dari Provider utama bersifat Dynamic IP Public. Untuk mengatasi masalah tersebut dilakukan penelitian melalui metode NDLC dengan penggabungan sistem protokol VPN L2TP/IPSec dan port forwarding yang ada di mikrotik VPS. VPN L2TP/IPSec yang dapat membantu menghubungkan dua router yang berbeda dalam satu jaringan private yang aman dan memungkingkan data terenkripsi dengan aman. Penggunaan VPS untuk mendapatkan Static Public IP sehingga dapat di port forward untuk membuka akses terhadap perangkat pada jaringan lokal agar dapat diakses melalui jaringan publik melalui remote address VPN. Hasil pengujian penggabungan VPN L2TP/IPSec dan port forwarding dapat digunakan Administrator dari jaringan publik untuk melakukan remote router mikrotik dan wireless access point pada jaringan Dynamic IP Public. Sehingga memudahkan Administrator dalam memonitoring jaringan secara realtime meningkatkan kualitas layanan internet.

Kata Kunci*—VPN, L2TP/IP Sec, Port Forwarding, Dynamic IP*

Abstract

One way that is done to maintain and improve the quality of services provided by XYZ Company, is that an administrator will monitor data traffic by accessing routers and access points to find out network conditions at any time. This can only be done by the Administrator while on the local network. The problem is that when an Administrator is on a public network, it cannot access the existing routers and access point devices. This is because the public IP obtained from the main Provider is Dynamic Public IP. To overcome this problem, research was carried out through the NDLC method by combining the L2TP / IPSec VPN protocol system and the port forwarding in the VPS proxy. The L2TP / IPSec VPN helps to connect two different routers in a secure private network and allows encrypted data to be safe during the communication process between routers. The use of VPS is to get a Static Public IP so that it can be ported forward to open access to devices on the local network so that it can be accessed through a public network via a VPN remote address. The results of testing the merging of VPN L2TP / IPSec and port forwarding, an Administrator from a public network can use a remote router and a wireless access point on a Dynamic IP Public network. Making it easy for Administrators to monitor networks in realtime and improve the quality of internet services.

Keywords*—3-5 VPN, L2TP/IP Sec, Port Forwarding, Dynamic IP*

1. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat membuat kebutuhan masyarakat dunia akan akses internet semakin tinggi. Perkembangan tersebut di ikuti munculnya berbagai unit usaha yang menyediakan jasa layanan internet. Setiap penyedia jasa layanan internet memiliki keunggulan dan kualitasnya masing-masing, terutama dalam hal pelayanan yang diberikan kepada *client*nya. Khsusunya pada Perusahan XYZ yang merupakan unit usaha yang bergerak dibidang penyedia jasa layanan internet. Saat ini Melayani pelanggan dengan berbagai macam kebutuhan dan penggunaan bandwidth yang berbeda-beda. Dalam menjaga dan meningkatkan kualitas layanan yang diberikan oleh Perusahaan XYZ kepada pelanggan, setiap saat administrator jaringan akan memonitoring lalulintas data dan kondisi perangkat jaringan.

Dalam memonitoring jaringan, administrator akan melakukan remote router *Mikrotik* melalui aplikasi winbox serta mengakses perangkat wireless *acces point* melalui *web browser*. Administrator dengan segera akan memberikan respon laporan dari pelanggan apabila terjadi gangguan dan melakukan analisa kesalahan untuk mengetahui kondisi jaringan yang ada. Hal tersebut saat ini hanya dapat dilakukan oleh seorang administrator *ketika* sedang berada dalam jaringan lokal. Dari wawancara yang dilakukan peneliti kepada administrator, diperoleh hasil bahwa ketika administrator sedang berada pada jaringan publik, maka tidak dapat melakukan remote router ataupun perangkat *Wireless Access Point* secara langsung. Administrator saat ini hanya menggunakan bantuan aplikasi *remote desktop* yang dianggap kurang efisien, dikarenakan membutuhan *bandwidth* yang besar saat melakukan remote dan sulit dioperasikan jika *remote* menggunakan *smartphone*. Hal tersebut disebabkan oleh IP publik yang didapatkan dari *Provider* utama bersifat tidak tetap atau *Dynamic IP Public*. Serta dengan berbagai perangkat *wireless* yang perlu diremote, membuat *IP Public static* bukan menjadi solusi utama, dikarenakan tarif sewa *IP Public Static* yang tinggi.

Berdasarkan latar belakang pada paragraph sebelumnya, maka dilakukan penelitian tentang "Penerapan Protokol *L2TP/IPsec dan Port* Forwarding untuk *Remote Mikrotik* pada Jaringan *Dynamic IP*" dengan memanfaatkan Layanan Mikrotik *VPS (Virtual Private Server)* yang bertujuan untuk mendapatkan *Static Public IP* yang berfungsi untuk *forwarding IP* sehingga dapat dilakukan *remote*. *VPN* (*Virtual Private Network*) yang memungkingkan dapat terkoneksi ke jaringan publik dengan menggunakan *tunnel* terenkripsi untuk terhubung dengan jaringan lokal. Penggunaan Protokol *L2TP (Layer 2 Tunneling Protocol)/IPSec (IP Security*) memberikan perlindungan ganda melalui otentikasi *L2TP* dan *IPSec* serta mendapat *virtual IP address* yang satu subnet dengan jaringan internal, sehingga *device* lain seperti berada pada *internal network*. Fungsi *port forwarding* adalah membuka akses terhadap perangkat pada jaringan lokal untuk dapat diakses melalui jaringan publik. *Port forwarding* akan mentranslasikan Remote address L2TP/IPsec yang didapatkan *Mikrotik client ke Static IP Public VPS* dengan penambahan port yang akan diakses. Dengan metode tersebut, *Administrator* hanya mengkonfigurasi *L2TP/IPSec client* di *Mikrotik* yang akan di*remote*. Dengan sistem ini diharapkan dapat membantu dan mempermudah *administrator* dalam melakukan *remote* perangkat jaringan melalui laptop maupun *smartphone* pada jaringan publik.

Hasil Penelitian [1] membandingkan 2 (dua) protocol VPN untuk Remote – site pada Mikrotik Router dan Protokol VPN yang digunakan adalah L2TP/IPsec dan OpenVPN. Dari penelitian tersebut dapat disimpulkan bahwa dengan menggunakan L2TP/IPSec atau OpenVPN pada Mikrotik router, dapat dilakukan komunikasi suara dan data antara 2 LAN yang berbeda jaringan. Pada L2TP/IPSec dan OpenVPN komunikasi suara tidak dapat dilakukan pengupingan. Untuk komunikasi VoIP L2TP/IPSec memiliki nilai jitter dan delay yang baik, sedangkan OpenVPN memiliki nilai packet loss dan troughput yang baik. Hasil penelitian sebelumnya [2] membahas tentang tunneling EoIP (Ethernet over IP) memanfaatkan jaringan internet melalui VPN untuk menghubungkan dua atau lebih suatu organisasi pada jaringan Dynamic IP dengan biaya relatif lebih murah. Hasil penelitian disimpulkan bahwa Fitur IP Cloud Mikrotik atau DDNS remote merupakan fitur yang menjadi solusi EoIP VPN pada Jaringan berbasis Dynamic IP. Penelitian lai sebelumnya membangun VPN yang aman dengan menggunakan L2TP dan IP Sec

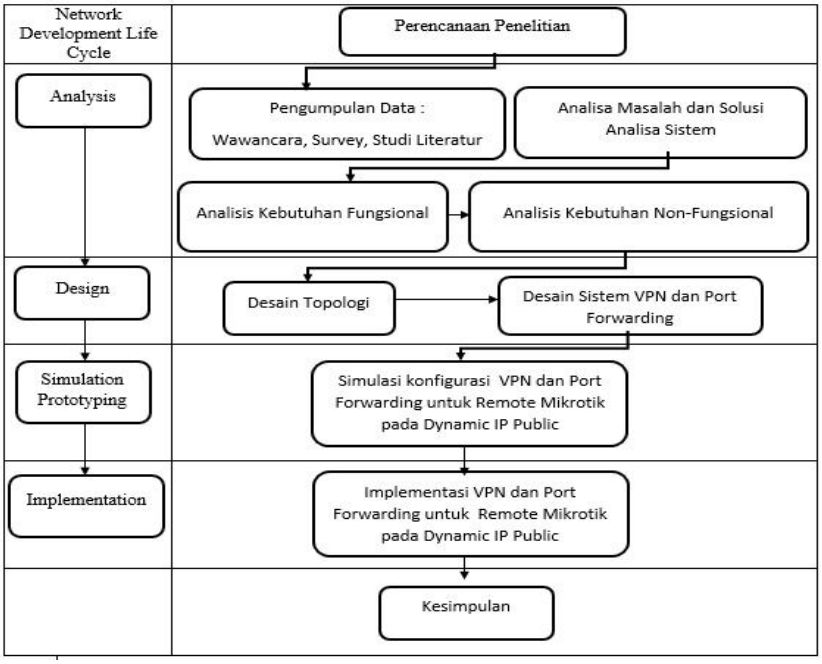
untuk memenuhi persyaratan transmisi keamanan data dalam meningkatkan Teknologi Keamanan VPN. Hasil penelitian menunjukkan bahwa Solusi VPN yang aman harus dapat mengautentikasi pengguna dan dengan ketat mengontrol bahwa hanya pengguna yang berwenang yang dapat mengakses VPN, menunjukkan siapa dan kapan mengakses informasi apa [3]. Solusi VPN harus dapat menetapkan jaringan pribadi untuk alamat pengguna dan memastikan keamanan alamat, melewati Internet publik, data harus dienkripsi. Solusi VPN harus dapat menghasilkan dan memperbarui klien dan kunci enkripsi server. Pada penggunaan L2TP dan IPSec yang terintegrasi, hanya dapat saling mendukung untuk membangun enkapsulasi multi-protokol, tetapi juga untuk menyediakan otentikasi dan enkripsi VPN.

Penelitian yang lain yang dilakukan sebelumnya membahas tentang analisa Perbandingan Pengaruh Penggunaan Protokol Tunneling IP Security dengan Protokol Tunneling Layer 2 Tunneling Protocol terhadap Quality of Services Pada Jaringan Virtual Private Network. Hasil penelitian yang dapat disimpulkan dalam penelitian ini adalah bahwa penggunaan protokol tunneling VPN IPSec maupun L2TP menyebabkan terjadinya penurunan QoS [4]. Penurunan QoS yang terjadi sangat kecil untuk konfigurasi jaringan yang sama, sehingga pada dasarnya penggunaan protokol tunneling VPN IPSec maupun L2TP tidak membebani performa dari jaringan yang menggunakan protokol tunneling VPN IPSecurity maupun L2TP.

Penelitian lain membahas tentang Performa Protokol Routing OSPF dan BGP pada Jaringan VOIP MPLS dengan Tunelling L2TP/IPSec [5]. Hasil penelitian yang bias disimpulkan dalam penelitian ini adalah bahwa secara keseluruhan penerapaan MPLS VPN mampu meningkatkan Quality of Service (QoS) protokol routing OSPF pada jaringan VoIP, khususnya pada parameter throughput dan jitter. Peningkatan nilai throughput sebesar 3% dan perbaikan jitter sebesar 26%. Selanjutnya perlu dilakukan traffic engineering pada jaringan VOIP MPLS VPN.

2. METODE PENELITIAN

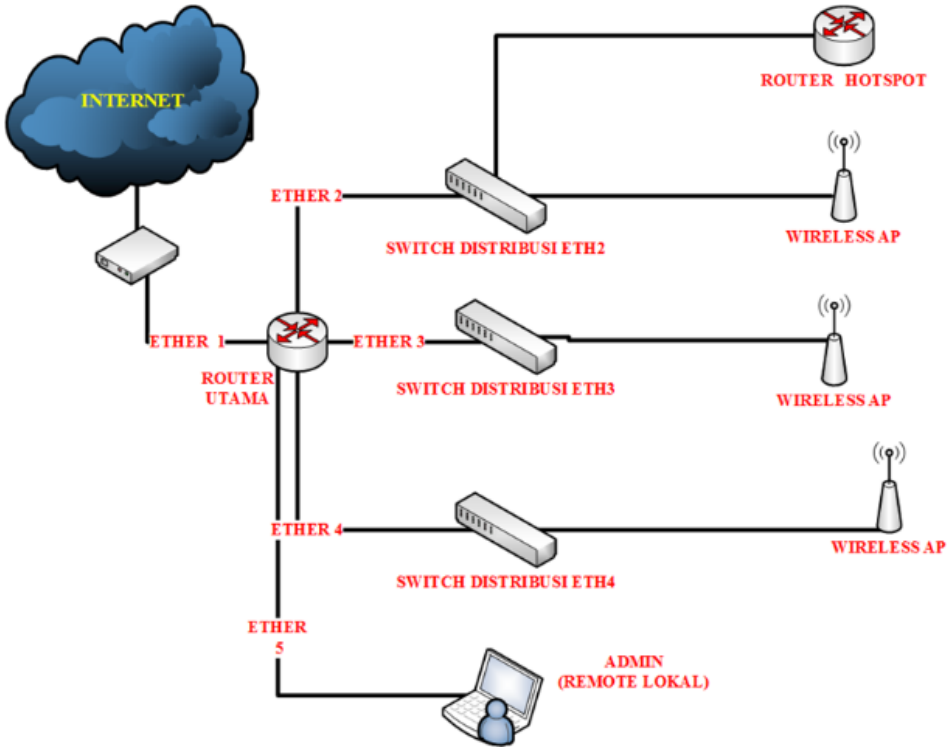
Pada penelitian ini menggunakan beberapa tahapan penelitian dengan mengacu kepada metodologi Netwok Development Life Cycle (NDLC). Adapun tahapan penelitian disajikan pada Gambar 1.



Gambar 1. Tahapan Penelitian NDLC

2.1. Analisis

Dari analisis topologi jaringan Perusahaan XYZ yang terdiri dari modem Telkom sebagai *backbone* utama. Dari *Router* utama didistribusikan ke 3(tiga) buah *switch, Wireless Access Point, router hotspot,* serta terhubung ke komputer *admin*. *Wireless Access Point* terhubung ke masing-masing switch. Administrator terhubung langsung dengan *router* utama, sehingga dapat melakukan *remote* terhadap perangkat jaringan yang ada di Jaya Network. *Router* untuk *hotspot* terhubung melalui "*switch* distribusi ether2". Detail topologi ditunjukan pada Gambar 2.



Gambar 2. Topologi jaringan Perusahaan XYZ

Dari identifikasi masalah dan topologi yang berjalan pada jaringan Perusahaan XYZ, maka dilakukan pengujian remote melalui jaringan publik dengan menggunakan aplikasi winbox untuk *remote Mikrotik* dan *web browser* untuk *remote Wireless Access Point.* Pengujian jaringan dilakukan menggunakan topologi atau sistem yang sudah berjalan sebelumnya, sehingga akan didapatkan hasil perbandingan sebelum dan sesudah sistem diterapkan. Adapun data masalah yang dihadapi sebagai berikut:

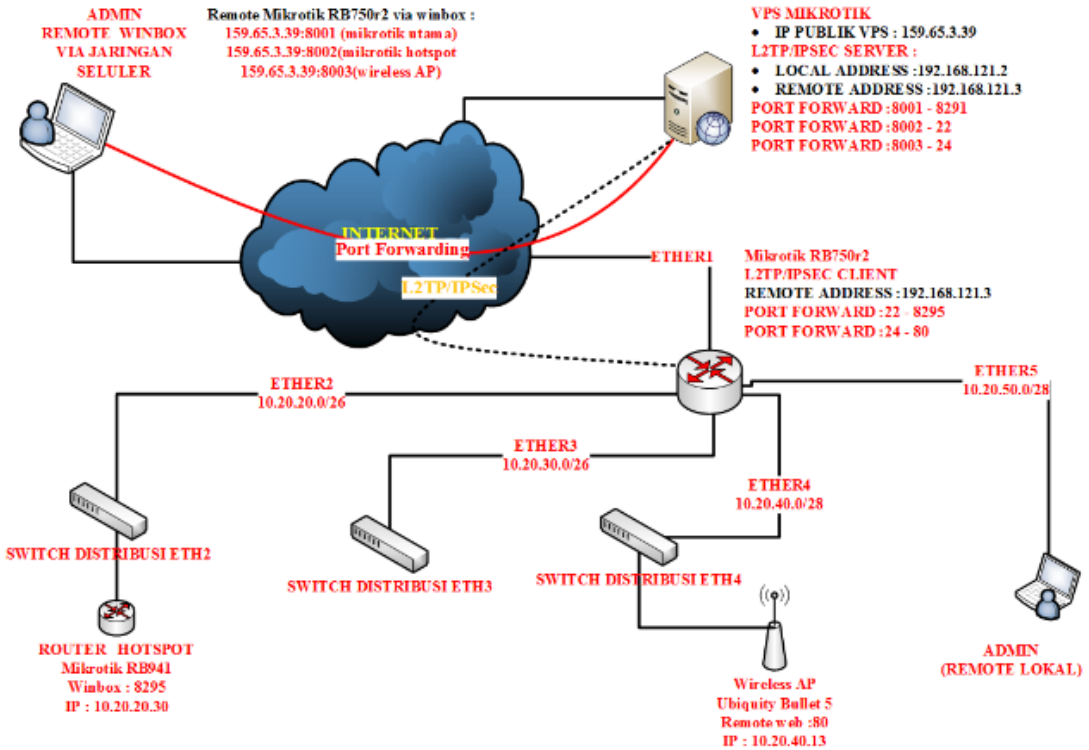
1. IP Publik yang didapatkan dari *Provider* Utama bersifat *Dynamic IP Public*. *Administrator* akan kesulitan untuk mer*emote router* dari jaringan publik, karena IP Publik yang tidak tetap.
2. *Administrator* hanya dapat mengakses atau meremote perangkat *Wireless Access Point* melalui jaringan lokal, dikarenakan IP yang digunakan adalah IP lokal dan belum adanya *rule* untuk memforward IP lokal *Wireless* AP ke jaringan publik.
3. Terdapat metode remote pada *Dymanic IP Public* menggunakan *DDNS(Dymanic Domain Name System)* dan *IP Cloud* pada *Router Mikrotik* tetapi tidak dapat berjalan dengan baik pada jaringan *Dynamic IP*.

Solusi terhadap masalah untuk remote mikrotik pada jaringan *Dynamic IP*. Dari hasil uraian dan data yang telah dikumpulkan, maka dapat ditemukan sebuah solusi yaitu sebagai berikut:

1. Dalam mengatasi *Dymanic IP Public* diperlukan sebuah *server* yang memiliki *Static IP Public* sebagai penghubung antara *router* yang akan di*remote* dan *client (admin).*
2. Merancang bangun sebuah jalur *private* antara *VPN Server* dan *VPN Client* menggunakan protokol *L2TP/IPSec*.
3. Merancang *rule firewall NAT* untuk membuka akses terhadap perangkat jaringan lokal untuk dapat diakses melalui jaringan publik.

2.2. Perancangan

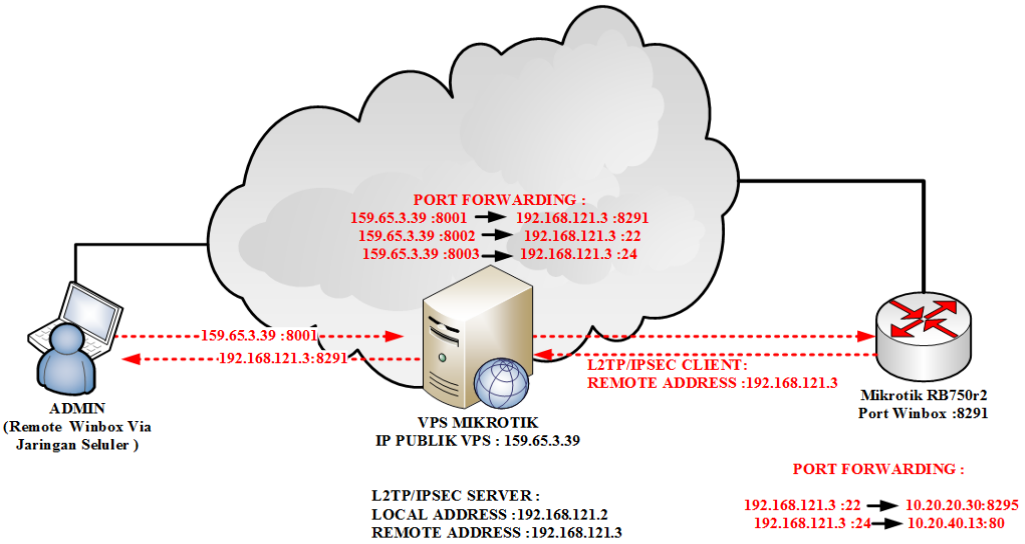
Dengan analisis dan solusi yang telah dilakukan, selanjutnya adalah membuat rancangan topologi sistem dengan menambahkan rule pada *Router Mikrotik* utama dan tidak merubah topologi secara fisik. *Administrator* lokal menggunakan ether 5(lima) untuk mengakses router dan perangkat *Wireless AP* melalui jaringan lokal. Sehingga menggunakan topologi dan *IP Address* yang sudah berjalan. Pada rancangan ini, perangkat yang diijinkan oleh pihak Jaya Net untuk dilakukan *remote* melalui jaringan publik terdiri dari *router* utama, *router hotspot* dari ether 2(dua), dan *Wireless AP* dari ether 4(empat). Rancangan topologi sistem ditunjukkan pada Gambar 3.



Gambar 3. Rancangan Topologi Sistem

Pada Gambar 3, dalam perancangan ini menggunakan protokol *VPN L2TP/IPSec Server* yang terpasang di *Mikrotik VPS* dan *L2TP/IPSec Client* pada *Mikrotik* yang akan di*remote* melalui jaringan publik. Penggunaan layanan *Mikrotik VPS* untuk mendapatkan *Public IP Static* sebagai *bridge* antara admin yang akan melakukan *remote* dengan *Mikrotik* Lokal pada jaringan *Dynamic IP Public*. Parameter yang penting adalah pembuatan *Local Address* dan *Remote Address* yang akan ditambahkan secara otomatis ketika koneksi *L2TP* terbentuk dan sebagai *gateway* untuk komunikasi. *Remote Address* adalah *IP Private* yang didapatkan oleh *Mikrotik Client* atau *L2TP/IPSec Client*.

Penggunaan *Port Forwarding* digunakan untuk meneruskan atau mengijinkan *Admin* untuk mengakses *router Mikrotik* utama melalui mekanisme seperti yang ditunjukan pada Gambar 4.



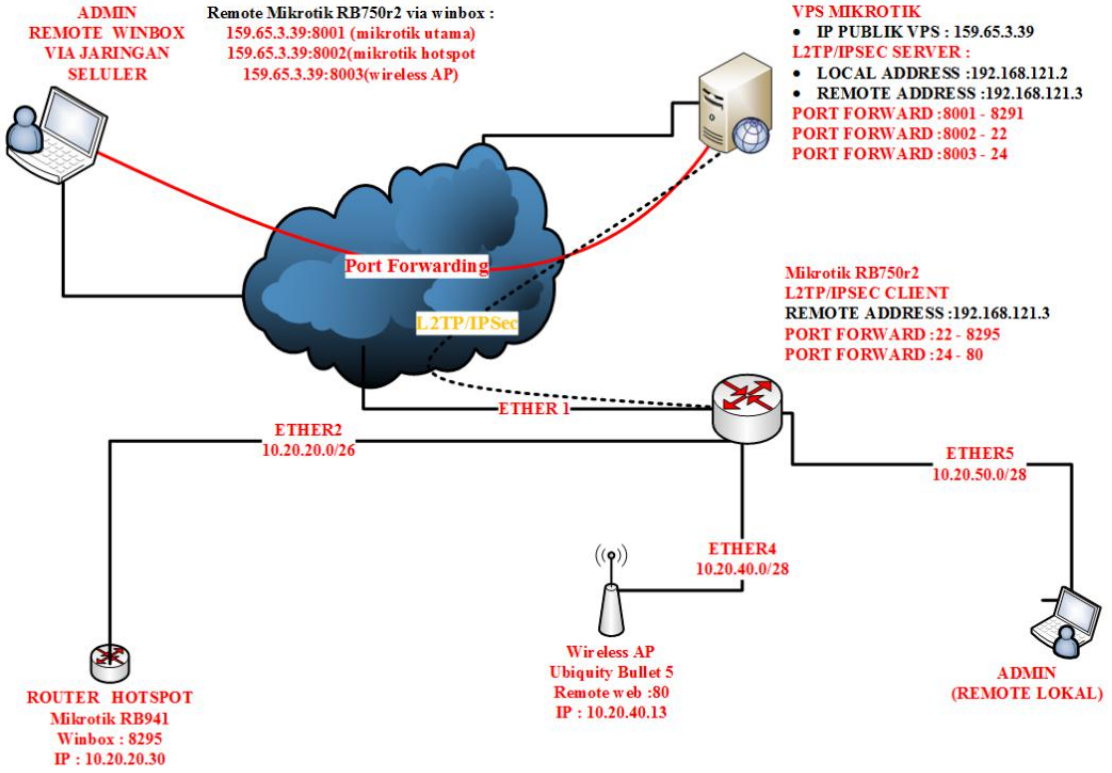
Gambar 4. Mekanisme remote

Keterangan dari Gambar 4 adalah sebagai berikut:

1. *Admin* akan melakukan *remote* router melalui *Public IP Static VPS* dengan penambahan port.
2. *VPS* akan melakukan pengalihan *IP* Publik *VPS* dan *port* ke *Remote Address L2TP/IPSec* serta *port default winbox.*

2.3. Simulasi (Simulation Prototype)

Simulasi sistem ini menggunakan VPS dari Digital Ocean dan perangkat yang akan diremote via publik yaitu Mikrotik Routerboard RB750r2, Mikrotik RB941, dan Wireless AP Ubiquity Bullet 5 pada jaringan Dynamic IP Public. Hal-hal yang dilakukan peneliti sebelum implementasi adalah membuat simulasi dengan beberapa tahapan antara lain: Simulasi Topologi Sistem, Simulasi Konfigurasi VPS, Simulasi Kofigurasi VPN L2TP Server Pada Mikrotik VPS, Simulasi Konfigurasi Secret L2TP Server, Simulasi Konfigurasi IPSec Server, Simulasi Konfigurasi Port Forwarding Pada Mikrotik VPS, Simulasi konfigurasi pada router utama, Simulasi Konfigurasi pada router hotspot, Simulasi Penggantian port default winbox di Mikrotik hotspot, Simulasi Konfigurasi pada Wireless Access Point, Simulasi Konfigurasi L2TP Client, Simulasi Konfigurasi IPSec Client, Simulasi penggantian port default telnet, Simulasi konfigurasi port forwarding pada Mikrotik router utama, Simulasi Pengujian Sistem Remote Via Jaringan Publik *Simulasi.* Pada tahapan ini hanya akan ditampilkan Simulasi Topologi Sistem. Simulasi sistem remote ini menggunakan topologi yang ditunjukan pada Gambar 5.



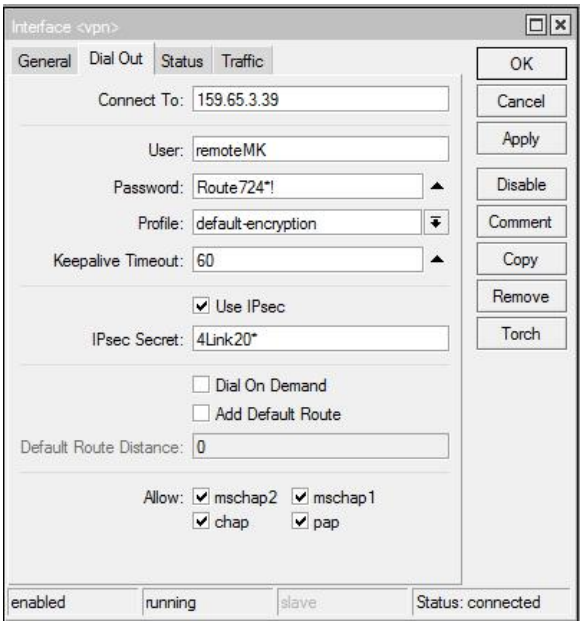
Gambar 5. Topologi Simulasi

2.4 Implementasi

Implementasi ini menggunakan topologi dan perangkat yang sudah ada pada jaringan di Perusahaan XYZ. Perangkat yang dizinkan untuk dilakukan implementasi sistem *remote* adalah Mikrotik RB750r2 sebgai router utama, Mikrotik RB133 sebagai router hotspot, Ubiquity Airgrid M5HP 23db sebagai *Wireless Access Point*. Dalam implementasi ini, menggunakan Mikrotik VPS dan konfigurasi sebelumnya yang digunakan pada tahap simulasi. Sehingga hanya melakukan konfigurasi disisi Mikrotik dan *Wireless Access Point* yang berada di jaringan Perusahaan XYZ. Berikut implementasi konfigurasi L2TP/IPSec dan *port forwarding* pada jaringan Perusahaan XYZ.

2.4.1 Implementasi Konfigurasi L2TP Client

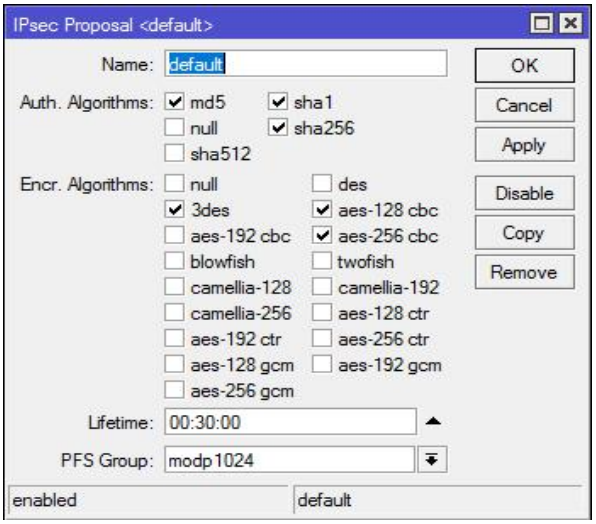
Konfigurasi pada Perangkat Mikrotik yang akan d*iremote* melalui jaringan *public*. Konfigurasi sesuai dengan *IP Public* VPS dan *Secret* yang telah dibuat pada L2TP *Server* di Mikrotik VPS. Konfigurasi L2TP *Client* ditunjukan pada Gambar 6.



Gambar 6. Konfigurasi L2TP Client Mikrotik

2.4.2 Implementasi Konfigurasi IPSec Client

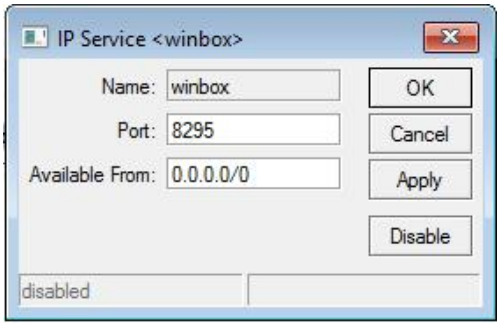
Konfigurasi proposal IPSec disesuaikan dengan Proposal IPSec *Server* sebelumnya. Konfigurasi Proposal IPSec *Client* ditunjukan pada Gambar 7.



Gambar 7. Konfigurasi Proposal IPSec Client

2.4.3 Implementasi Penggantian port default winbox di Mikrotik hotspot

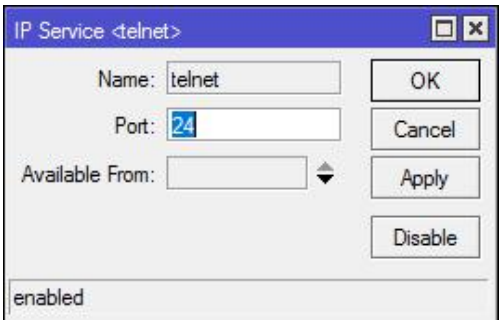
Konfigurasi penggantian *port default* Winbox pada Mikrotik hotspot dapat dilihat pada Gambar 8.



Gambar 8. Penggantian port default winbox

2.4.4 Implementasi penggantian port default telnet Mikrotik Utama

Penggantian *port default* telnet pada router Mikrotik utama. Konfigurasi telnet dapat dilihat pada Gambar 9.



Gambar 9. Penggantian port default telnet

2.4.5 Implementasi Konfigurasi port forwarding pada Mikrotik utama

Detail konfigurasi *port forwarding* masquerade di router Mikrotik utama ditunjukan pada Gambar 10.

Gambar 10. NAT masquerade vpn

Port forwarding untuk mengijikan akses dari luar menuju ke Mikrotik router hotspot. Konfigurasi *port forward* router hotspot di router utama ditunjukan pada Gambar 11.

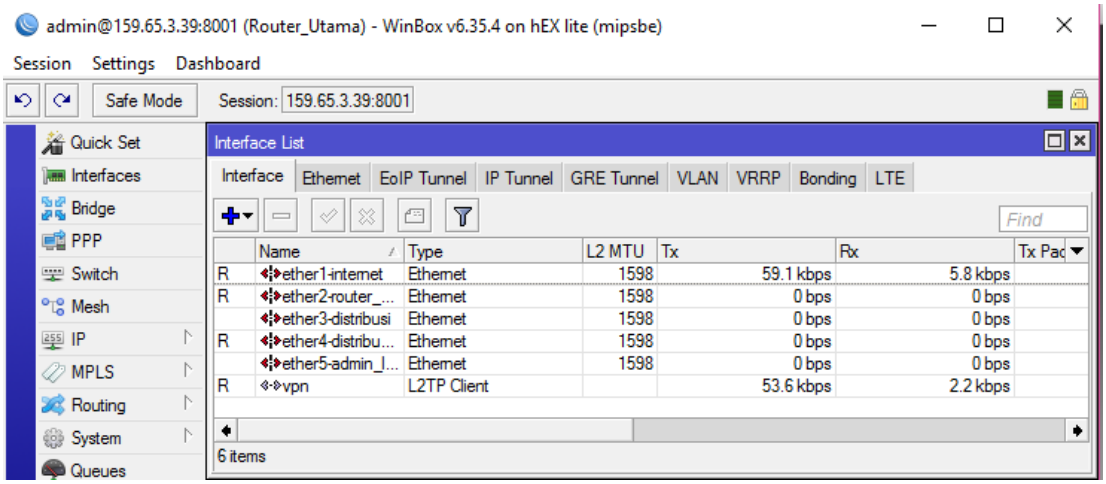
Gambar 11. Port forwarding router hotspot diMikrotik utama

Konfigurasi *port forwarding* Wireless Access Point agar dapat diremote melalui jaringa publik. Konfigurasi *port forward Wireless Access Point* di router utama ditunjukan pada Gambar 12.

Gambar 12. port forwarding wireless AP repeater di Mikrotik utama

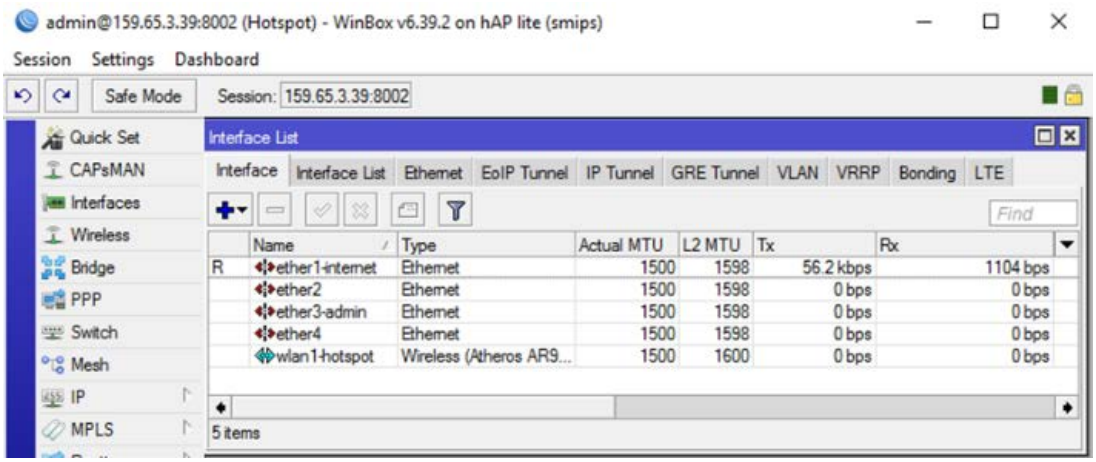
3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan serangkaian pengujian yang telah dilakukan oleh peneliti. Pengujian ini dilakukan menggunakan sistem remote menggunakan perangkat Laptop yang terhubung dengan jaringan internet seluler. Pengujian remote terdiri dari tiga (3) buah perangkat, yaitu router utama (Mikrotik RB750r2), router hotspot (Mikrotik RB941), Wireless AP (Ubiquity Bullet 5). Router utama atau Mikrotik RB750r2 harus terhubung dengan internet dan VPN L2TP/IPSec Server. Admin akan melakukan remote melalui Aplikasi Winbox untuk perangkat Mikrotik dan web browser untuk perangkat wireless AP. Parameter yang digunakan pada winbox adalah IP Address dan Port serta username, password. Pengujian remote router utama melalui jaringan publik ditunjukan pada Gambar 13.



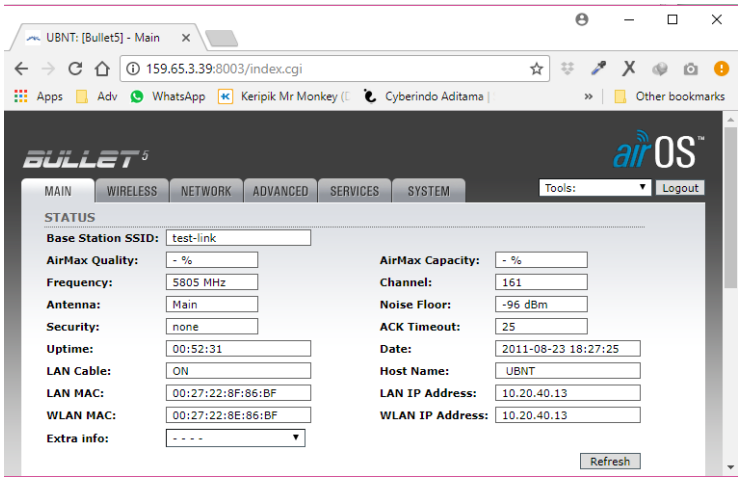
Gambar 13. Pengujian remote mikrotik utama

Gambar 13 menunjukkan bahwa *remote Mikrotik* dan perangkat *Wireless Access Point* dapat dilakukan pada Jaringan *Dynamic IP Public.* Pengujian selanjutnya adalah melakukan *remote Mikrotik router hotspot* yang berada di belakang *router* utama. Pengujian *remote Mikrotik router hotspot* ditunjukan pada Gambar 14.



Gambar. 14. Pengujian remote mikrotik hotpsot

Gambar 14 menerangkan bahwa Perangkat *Mikrotik* dan *Wireless Access Point* yang berada di Perusahaan XYZ dapat dilakukan *remote* secara publik. Kemudian Pengujian *remote Wireless Access Point* menggunakan *web browser*. Pengujian *remote Wireless Access Point* ditunjukan pada Gambar 15.



Gambar 15. Pengujian remote wireless AP

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan, maka peneliti dapat mengambil kesimpulan, sebagai berikut:

1. Dengan menggunakan sistem *VPN L2TP/IPSec dan Port Forwarding, remote Mikrotik* dan perangkat *Wireless Access Point* dapat dilakukan pada Jaringan *Dynamic IP Public.*
2. Perangkat *Mikrotik* dan *Wireless Access Point* yang berada di Perusahaan XYZ yang sebelumnya tidak dapat diremote melalui jaringan pubik dikarenakan menggunakan *Dynamic IP Public* dari *Provider* Telkom, tetapi dengan adanya penerapan *VPN L2TP/IPSec* dan *port forwarding* dapat dilakukan *remote* secara publik.
3. Dapat meningkatkan kualitas pelayanan kepada client, dikarenakan ketika *Administrator* berada dijaringan publik masih dapat melakukan manajemen jaringan. Dengan begitu, *Administrator* akan menberitahukan kendala yang terjadi kepada *client*.
4. Dapat melakukan remote perangkat jaringan yang berada dibelakang router utama pada jaringan *Dynamic IP Public*.

5. Konfigurasi *port* pada setiap perangkat yang dapat mempermudah *administrator* dalam mengklasifikasikan perangkat yang akan *diremote.*
6. *VPS* yang *direinstall* dengan Sistem Operasi *Mikrotik Cloud Host Router* dapat digunakan sebagai *Bridge* antara *Mikrotik* yang terhubung di jaringan *Dynamic IP Public* dengan *Administrator* pada jaringan publik

5. SARAN

Dari penelitian ini terdapat saran yang dapat digunakan untuk melakukan pengembangan pada penelitian selanjutnya, sebagai berikut:

1. Sebagai bahan rujukan atau rekomendasi pada Perusahaan XYZ, bahwa ada metode yang lebih mudah dalam melakukan remote perangkat jaringan melalui jaringan publik.
2. Dapat dikembangkan untuk dapat melalukan remote monitoring CCTV melalui jaringan publik.
3. *Public IP Static VPS* dapat di*resolv* menggunakan nama domain, sehingga dapat mempermudah *Administrator* dalam mengingat suatu alamat.
4. Mengembangkan sistem registrasi perangkat yang akan diremote melalui *web management*, memanfaatkan *API (Aplication Programming Interface) Mikrotik*.

DAFTAR PUSTAKA

[1] Sahni, L., Munadi, R., Rumani., 2012, Perancangan, Implementasi, dan Analisa Perbandingan L2TP/IPsec VPN dengan OpenVPN pada Mikrotik Router, *Skripsi*, Fakultas Elektri dan Komunikasi, Telkom University, Bandung

[2] Mubarok D. F., 2016, Implementasi EoIP over VPN di Jaringan Berbasis Dynamic IP (Studi Kasus PT. Validata Teknologi), Universitas AMIKOM Yogyakarta.

[3] Fan, Y. Q., Li, Chi., Sun, C., 2012, Secure VPN Based on Combination of L2TP and IPSec, *Jurnal of Network*, No. 1, Vol. 7, Hal. 141-148

[4] Taofano, H., Sari, L. O., 2017, Analisa Perbandingan Pengaruh Penggunaan Protokol Tunneling IP Security dengan Protokol Tunneling Layer 2 Tunneling Protocol terhadap Quality of Services Pada Jaringan Virtual Private Network, *Jom FTEKNIK*, No. 1, Vol. 4.

[5] Susanto, B. M., Atmaji, E. S. J., 2017, Performa Protokol Routing OSPF dan BGP pada Jaringan VOIP MPLS dengan Tunelling L2TP/IPSec, *Seminar Nasional Hasil Penelitian 2017*, Jember.