ISBN: 978-623-91277-6-3

IMPLEMENTASI IP CLOUD DAN DEMILITARIZED ZONE (DMZ) UNTUK PENGONTROLAN ROUTER JARAK JAUH

Standy Oei
Jurusan Teknik Informatika, Fakultas ILKOM, Universitas Nusantara, Manado
E-mail: standy_oei@nusantara.ac.id

Abstract

Along with the development of science and technology, communication and information has become important requirement. The need for communication and information has penetrated into various sectors of human life. Various kinds of infrastructures have been built in order to support communication and information. One is the internet infrastructure. With the Internet, we can communicate and exchange the information quickly and actual. Because the Internet has an important role, it needs a good management. In the management of the Internet, usually every company/institution/office uses the router as a regulator. Where all of internet data Traffic is organized here. And to get a good quality of Internet, it requires the control of the router in Real Time. It means the router can be accessed and controlled at any time when needed or when there is a network/internet problem. For that reason, it is necessary to think how to control router remotely without time and place limitation. In this research, it tried to raise the case study of controlling router remotely, using Mikrotik RouterBoard and Telkom IndiHome Modem. Where there were IP Cloud feature on Mikrotik and DEMILITARIZED ZONE (DMZ) feature on Telkom IndiHome Modem, which allowed for controlling remotely. Although the controlled Router was under Network Address Translation (NAT) filter from Telkom IndiHome Modem.

Keywords: IP Cloud, DMZ, Mikrotik, IndiHome, NAT.

Abstrak

Seiring dengan perkembangan ilmu pengetahuan dan teknologi, komunikasi dan informasi telah menjadi kebutuhan penting. Kebutuhan akan komunikasi dan informasi telah merambah ke berbagai sektor kehidupan manusia. Berbagai macam infrastruktur telah dibangun dalam rangka menunjang komunikasi dan informasi. Salah satunya adalah infrastruktur Internet. Dengan Internet, kita bisa melaksanakan komunikasi dan pertukaran informasi secara cepat dan aktual. Dikarenakan Internet telah memegang peran penting, maka dibutuhkan adanya suatu pengelolaan yang baik. Dalam pengelolaan internet, biasanya setiap perusahaan/institusi/kantor menggunakan router sebagai alat pengaturnya. Dimana semua trafik data internet diatur disini. Dan untuk mendapatkan kualitas internet yang baik dibutuhkan adanya pengendalian/pengontrolan router secara real time. Dalam artian router bisa diakses dan dikendalikan setiap waktu ketika diperlukan ataupun ketika terdapat permasalahan jaringan/internet. Untuk itulah, maka perlu dipikirkan bagaimana caranya pengontrolan jarak jauh router bisa

ISBN: 978–623–91277–6–3

dilakukan tanpa terbatas waktu dan tempat. Pada penelitian ini, mencoba mengangkat studi kasus pengontrolan jarak jauh router, menggunakan RouterBoard Mikrotik dan Modem Telkom IndiHome. Dimana terdapat fitur IP Cloud pada Mikrotik dan Fitur DEMILITARIZED ZONE (DMZ), yang memungkinkan terjadinya pengontrolan jarak jauh ini. Meskipun router yang dikendalikan berada dibawah filter Network Address Translation (NAT) dari Modem Telkom IndiHome.

Kata kunci: *IP Cloud, DMZ, Mikrotik, IndiHome, NAT*.

1. PENDAHULUAN

Tidak bisa dipungkiri lagi bahwa kebutuhan akan komunikasi dan informasi sudah menjadi hal yang sangat penting. Hal ini dikarenakan pembangunan suatu bangsa tidak akan lepas dari kebutuhan akan komunikasi dan informasi. Dengan adanya infrastruktur komunikasi dan informasi, misalnya *internet*, membuat proses pertukaran/adopsi ilmu pengetahuan dan teknologi menjadi semakin mudah. Hal ini dikarenakan sumber ilmu pengetahuan dan teknologi tidak lagi terbatas oleh fisik, ruang, maupun waktu. Setiap orang yang berada di belahan bumi manapun bisa mengakses maupun berperan dalam perkembangan ilmu pengetahuan dan teknologi tersebut. Selain pemanfaatan untuk perkembangan ilmu pengetahuan dan teknologi, *internet* telah luas digunakan dalam berbagai aspek/sektor kehidupan manusia. Misalnya di bidang perdagangan (*e-commerce*), pemerintahan (*e-government*), pendidikan (*e-learning*), dan lain sebagainya. Selain untuk bidang yang serius, *internet* bahkan telah digunakan untuk kegiatan bersosialisasi (sosial media). Banyak media sosial telah tumbuh dan digemari dengan memanfaatkan pertumbuhan *Internet*, misalnya *facebook*, *instagram*, *twitter*, dan lain sebagainya. Belum lagi pemanfaatan untuk komunikasi *online*, seperti *WhatsApp*, *Line*, maupun *Telegram*. Dengan begitu, *internet* bisa dikatakan telah memegang kendali hampir di semua aspek kehidupan manusia.

Karena begitu pentingnya *internet*, maka perlu dilakukan suatu pengaturan ataupun pengendalian yang baik. Dalam pengaturan ataupun pengendalian *internet*, setiap perusahaan/institusi/kantor menggunakan *router* sebagai alat pengaturnya. Dengan *router* kita bisa mengatur trafik data *internet* yang sedang digunakan. Baik dengan fungsi *Firewall* (*Filter Rules*, *NAT*, *Mangle*), *Routing*, *Bridging*, *Proxy*, *DNS*, *DHCP*, *Bandwidth Management* (*Simple Queue*, *Queue Tree*) dan lain sebagainya. Dengan *Router* kita bisa mengendalikan kualitas maupun kuantitas data *Internet* yang akan dilewatkan sesuai dengan kebutuhan.

Dikarenakan fungsi yang penting dari *router* dalam mengontrol *internet*, maka diperlukan ketersediaan akses terhadap *router* secara *real time*. Dalam artian *router* bisa diakses kapan saja ketika dibutuhkan ataupun ketika terdapat permasalahan jaringan/*internet*. Untuk bisa mengakses *router* ketika masih terkoneksi ke jaringan lokal *router* tersebut bukanlah menjadi hal yang sulit. Yang menjadi kendala adalah "Bagaimana caranya mengakses *router* ketika kita berada di luar jaringan lokal *router*? Dimana mungkin saja *router* tersebut masih berada dibawah filter *Network Address Translation* (NAT) dari suatu *Modem Internet*".

ISBN: 978–623–91277–6–3

Dalam penelitian ini akan mencoba membahas bagaimana caranya mengakses/mengontrol *router* dari luar jaringan lokal *router* atau lewat *internet*, menggunakan Fungsi/Fitur *IP Cloud* pada *Router* Mikrotik dan Fungsi/Fitur *DEMILITARIZED ZONE* (DMZ) pada *Modem* Telkom IndiHome. Walaupun *Router* Mikrotik yang akan dikendalikan masih berada dibawah Filter NAT dari *Modem* Telkom IndiHome.

2. METODE PENELITIAN

Penelitian dilakukan dalam bentuk pengujian empiris, dimana dilakukan percobaan/observasi untuk mendapatkan hasil pembuktian. Percobaan-percobaan yang dilakukan adalah untuk menggabungkan fitur *IP Cloud* pada *Router* Mikrotik dan Fitur DMZ pada *Modem* Telkom IndiHome untuk memperoleh fungsi pengontrolan jarak jauh *router*.

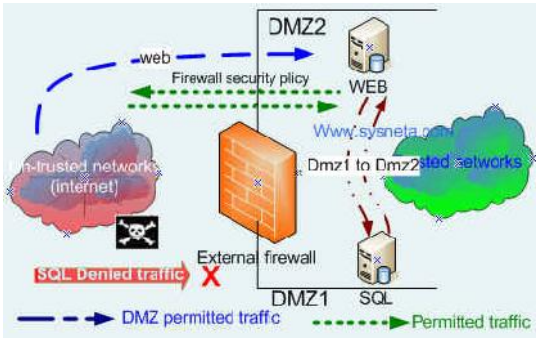
2.1 *Demilitarized Zone* (DMZ)

Untuk menghubungkan jaringan *private*/*business* kita dengan jaringan *public* seperti jaringan *internet*, tentulah kita harus mengatur aliran *traffic* paket dengan menggunakan perangkat *firewall* yang diperkuat dengan *policy* keamanan. Dengan *firewall*, semua *traffic* dipaksa melalui satu *check point* tunggal yang terkonsentrasi dimana semua *traffic* dikendalikan, diauthentikasi, di-*filter*, dan di-*log* menurut *policy* yang diterapkan pada *firewall* tersebut. Dengan cara ini, kita bisa mengurangi secara signifikan, akan tetapi tidak menghilangkan *traffic* yang tidak kita harapkan yang akan mencapai jaringan *private* kita.

Kemudian bagaimana kalau kita akan meletakkan beberapa *public resources* (seperti *server web*) yang memang disediakan untuk bisa diakses oleh *user* umum dari *Internet* dengan aman? Kita bisa menyediakan fasilitas *web-server* atau *mail-server* yang bisa diakses oleh *public* tanpa harus membiarkan mereka bisa leluasa masuk atau mengakses jaringan *private corporate* kita dengan jalan memberikan segmentasi pada *system firewall* kita, dengan suatu jaringan perimeter atau lebih dikenal dengan *Firewall* dengan DMZ.

Firewall DMZ atau jaringan perimeter adalah jaringan *security boundary* yang terletak di antara suatu jaringan *corporate/private* LAN dan jaringan *public* (*internet*). *Firewall* DMZ ini harus dibuat jika perlu dibuat segmentasi jaringan untuk meletakkan *server* yang bisa diakses *public* dengan aman tanpa harus bisa mengganggu keamanan sistem jaringan LAN di jaringan *private* kita. Perimeter (DMZ) *network* di-*design* untuk melindungi *server* pada jaringan LAN *corporate* dari serangan *hackers* dari *internet*.

Gambar 1 menunjukkan diagram dari *firewall* yang menggunakan dua jaringan DMZ.



Gambar 1. *External Firewall* dengan Dua DMZ

Jika ada kebutuhan untuk menggunakan jaringan segmentasi, bisa diterapkan beberapa jaringan DMZ dengan kebijakan tingkat keamanan yang berbeda. Seperti terlihat pada Gambar 1, pembangunan aplikasi untuk keperluan *extranets*, *intranet*,

ISBN: 978–623–91277–6–3

dan *web-server hosting* dan juga *gateway* untuk keperluan *remote* akses.

Perhatikan diagram DMZ pada Gambar 1, *traffic user* dari *internet* hanya dapat mengakses *web-server* yang diletakkan pada jaringan DMZ2. Mereka tidak bisa mengakses server SQL yang diletakkan pada jaringan DMZ1. Akan tetapi kedua *server* baik *web-server* (yang ada di DMZ2) dan *SQL-server* (yang ada di DMZ1) mempunyai akses untuk bisa saling berkomunikasi. *User* dari *internet* tidak boleh mengakses *SQL server* maupun mengakses jaringan internal/*private* kita. Sehingga harus diterapkan kebijakan keamanan pada *firewall* yang memenuhi kebutuhan tersebut.

Firewall DMZ dapat diimplementasikan tepat pada *border corporate* LAN yang lazim mempunyai tiga jaringan *interface*:

a. *Interface Internet*: *Interface* ini berhubungan langsung dengan *internet* dan *IP address*-nya pun juga *IP public* yang ter-register.
b. *Interface Private* atau *Interface Intranet*: adalah *interface* yang terhubung langsung dengan jaringan *corporate* LAN dimana diletakkan *server-server* yang rentan terhadap serangan.
c. Jaringan DMZ: *Interface* DMZ ini berada didalam jaringan *internet* yang sama sehingga bisa diakses oleh *user* dari *internet*. *Resources* publik yang umumnya berada pada *firewall* DMZ adalah *web-server, proxy*, dan *mail-server*.

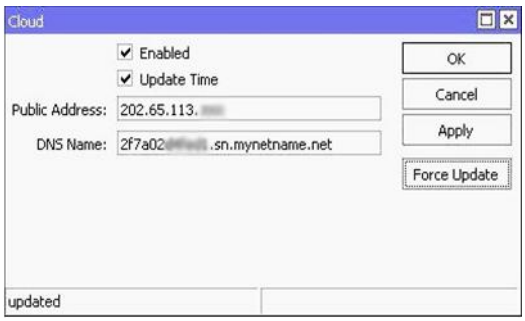
Ada banyak *wireless router* yang biasa dipakai untuk jaringan rumahan atau kantoran kecil yang dilengkapi dengan fitur DMZ, seperti WRT610N dari Linksys. *Wireless router* yang dilengkapi dengan fitur DMZ ini memungkinkan untuk diletakkan satu komputer yang bisa di-*expose* ke *internet* dengan tujuan tertentu, seperti untuk *online gaming* atau *video-conference*. DMZ *hosting* ini meneruskan semua *ports* pada saat yang bersamaan kepada satu PC. Fitur *forward port* ini lebih aman, sebab dia hanya membuka *port-port* yang ingin dibuka saja, sementara *hosting* DMZ membuka semua *port* dari satu komputer, meng-*expose* komputer kepada *internet*. Misal pada WRT610N Linksys bisa meng-*configure* satu PC atau *game console* untuk keperluan *Online Gaming*, sehingga terpisah dari jaringan komputer *private* anda. Anda bisa mengakses utilitas *Web-based* dari WRT610N ini dan masuk ke menu *Application* > DMZ untuk bisa meng-*enable* fitur DMZ ini. *Enable* dulu fitur DMZ dan kemudian lakukan konfigurasi-nya. Pilih *IP address* atau masukkan *IP address* tertentu secara *manual* dari komputer yang ada di *internet* yang dibolehkan masuk mengakses PC yang ada pada jaringan. Anda juga perlu memasukkan *IP address* atau *MAC address* dari PC/*Game Console* yang anda ingin *expose* di i*nternet* dan bisa diakses dari *Internet*. (Hariono, 2017)

2.2 IP Cloud

Dengan habisnya IPv4 membuat *IP Public* semakin mahal. Untuk berlangganan *IP Public static* tentu akan memaksa kita untuk merogoh kocek lebih dalam. Sedangkan *IP Public dynamic* biasanya lebih murah. Dengan harga murah *IP Public dynamic*, terkadang menimbulkan kesulitan tersendiri bagi *admin* jaringan yang hendak membuat *router* untuk menyediakan *service* yang bisa diakses dari jaringan *Internet* menggunakan *IP Public*. Misalnya *Virtual Private Network* (VPN), atau hanya sekedar me-*remote router* dari *Internet*. Akan tetapi, *IP Public Dynamic* sudah tidak lagi menjadi masalah di MikroTik RouterOS mulai versi 6.14. Di versi ini terdapat fitur baru yang bernama *IP Cloud*. Fitur ini menyediakan

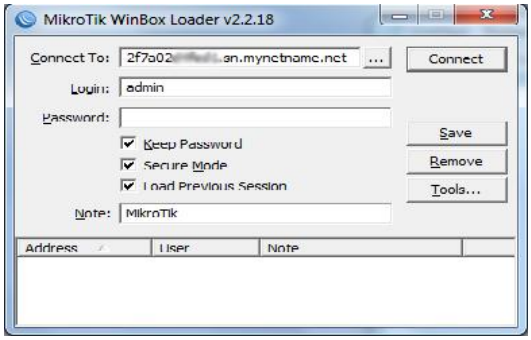
ISBN: 978–623–91277–6–3

layanan yang bisa dikatakan hampir sama seperti *service Dynamic Domain Name System* (DDNS) yang banyak tersedia di *internet*. Dengan fitur ini, *service router* yang sebelumnya diakses dengan *IP Public*, diganti dengan DNS yang disediakan oleh MikroTik.com. Dan ketika *IP Public* berubah, *router* akan melakukan *update* ke MikroTik.com sehingga *service router* tetap bisa diakses dengan DNS yang telah diberikan sebelumnya. Jika sebelumnya kita bisa menggunakan layanan DDNS dari pihak ketiga, kita membutuhkan *script* yang cukup rumit agar *router* melakukan *update* ke penyedia DDNS. Dengan fitur *IP Cloud*, cukup masuk ke menu IP --> Cloud, kemudian centang "*Enabled*" dan selesai. Gambar 2 berikut akan memperlihatkan Tampilan Fitur *IP Cloud*.



Gambar 2. Tampilan Fitur *IP Cloud*

Sebelum menjalankan fitur *IP Cloud* ini, pastikan *router* sudah terkoneksi ke *internet*, agar *router* dapat melakukan *request* DNS ke *IP Cloud Server*. Jika statusnya sudah "*updated*", maka kita bisa menggunakan nama *Domain* untuk *remote router* atau mengakses *service* yang dijalankan oleh *router* seperti VPN dari jaringan *internet*. Setiap menit *router* akan selalu memeriksa *outgoing IP Router* dan akan melakukan *update* IP ke *IP Cloud Server*. Dengan begitu, walau *IP public router* berubah-ubah, kita tetap bisa *remote* atau VPN ke *router* menggunakan nama domain yang sama. Gambar 3 memperlihatkan Contoh *Remote Router via* WinBox dengan menggunakan *Domain*.



Gambar 3. Contoh *Remote Router via* WinBox dengan menggunakan *Domain*

Agar fitur *IP Cloud* ini dapat berjalan dengan baik, pastikan *router* terkoneksi secara langsung dengan i*nternet*, sehingga *IP public* terpasang di *router*. Jika *router* hanya memiliki *IP private* maka akan muncul informasi "*DDNS server received request from IP 202.65.xxx.x but your local IP was 192.168.128.102; DDNS service might not work.*" Untuk saat ini fitur *IP Cloud* hanya *support* untuk IPv4 dan belum *support* IPv6.

Selain *remote router*, bisa juga untuk melakukan dial VPN, karena ternyata dial VPN, misalnya PPTP, ternyata juga bisa menggunakan *domain*. Gambar 4 memperlihatkan Contoh Implementasi *Dial VPN* menggunakan *Domain*. Selain dapat *update Dynamic DNS*, fitur *IP Cloud* juga bisa dimanfaatkan untuk *update* pengaturan waktu pada *router* jika *NTP Client* tidak aktif. Caranya, selain centang "*Enabled*" pada menu *IP Cloud*, centang juga "*Update Time*".

Gambar 4. Contoh Implementasi *Dial VPN* Menggunakan *Domain*

ISBN: 978–623–91277–6–3

Dan perlu diketahui, fitur *IP Cloud* tersedia mulai RouterOS versi 6.14, dan tidak ada di routerOS sebelum 6.14. Format nama *domain* yang diberikan berdasarkan *serial number* RouterBoard yang kita gunakan, jadi *format domain* ditulis seperti berikut:

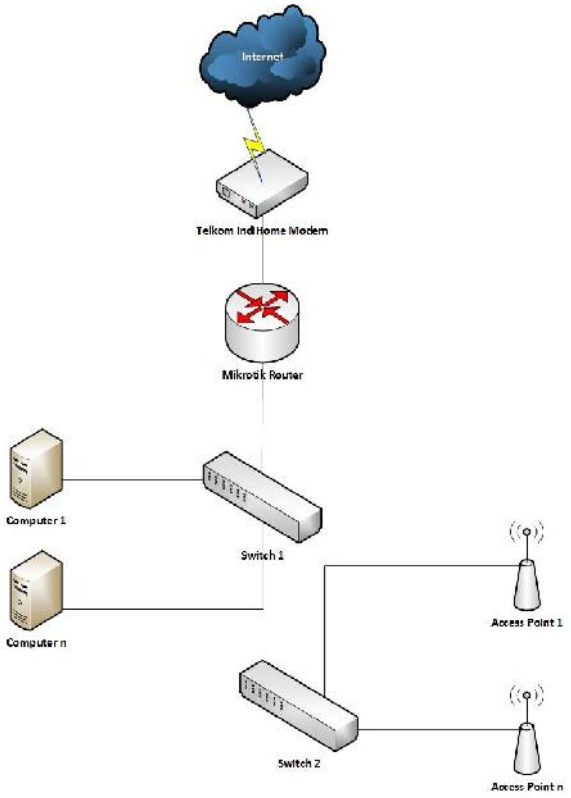
[SN RouterBoard].sn.mynetname.net

SN disini maksudnya *serial number*, jadi DNS di-*generate* berdasarkan *serial number* yang terdapat pada *router*. Perlu diketahui bahwa fitur *IP Cloud* ini hanya *support* untuk produk *RouterBoard*, dan belum *support* untuk produk x86. Perlu diketahui, *router* MikroTIk akan menggunakan protokol UDP dengan *port* 39752 untuk melakukan *request* atau *update IP Address* ke *server IP Cloud*. Pastikan jika Anda membuat *rule firewall filter*, tidak melakukan *block* terhadap protokol dan *port* tersebut. (Citraweb Nusa Infomedia, 2017).

2.3 Model Penelitian

Pada penelitian ini mengambil model contoh kasus *router* yang berada dibawah Filter NAT dari *Modem*. Dimana *interface* pada *router* yang terhubung *internet* tidak mendapatkan *IP Public* secara langsung, tetapi hanya mendapatkan IP Lokal/*Private* dari DHCP *Modem*. Gambar 5 memperlihatkan skema topologi jaringan yang diteliti.

Oleh karena IP yang didapat *router* bukanlah *IP Public*, maka proses pengendalian jarak jauh ini tidak bisa dilakukan. Untungnya masih ada Fitur DMZ pada *Modem*. Dengan Fitur DMZ, *modem* akan melakukan *bypass interface internet* dengan *interface* yang dimiliki oleh *router*. Seolah-olah *interface router* adalah *interface* yang terkoneksi langsung ke *internet* sehingga mempunyai *IP Public* yang sama dengan *interface modem* yang terkoneksi ke *internet*. Semua paket/*traffic* yang menuju *IP Public* dari *interface internet modem*, akan diteruskan ke *interface*-nya *Router*. Dengan begitu *router* akan ter-*expose* dan bisa di akses dari *internet*.



Gambar 5. Skema Topologi Jaringan yang diteliti

Yang menjadi kendala berikutnya adalah masalah *IP Public* yang terus berubah-ubah atau *Dynamic IP Public*. Dimana untuk bisa mengakses *router*, kita perlu mengetahui dengan tepat/pasti *IP Public* dari *router* kita. Untuk itu, kita bisa menggunakan fitur *IP Cloud* dari *Router* Mikrotik. Dimana kita tidak perlu mengingat nomor-nomor dari *IP Public* yang terus berubah-ubah, tetapi cukup menggunakan fitur ini untuk menyimpan *IP Public* ini ke dalam *server* MikroTik.com. Sebagai gantinya MikroTik.com memberikan sebuah DNS yang bisa kita akses, yang menyimpan/merepresentasikan alamat *IP Public Router* Mikrotik kita.

ISBN: 978–623–91277–6–3

3. HASIL DAN DISKUSI

Pada penelitian ini, hal yang pertama kali dilakukan ialah proses konfigurasi pada *Modem* Telkom IndiHome dan *Router* Mikrotik. Sebelum melakukan konfigurasi pada *Modem* Telkom IndiHome, kita akan melihat *Device Information* dari *Modem* tersebut. Dari konfigurasi bawaan (*default*) yang ada pada *Modem* Telkom IndiHome, kita bisa melihat bahwa fitur *filter* NAT telah diset aktif. Dari pengamatan yang ada, diperoleh informasi bahwa secara *default Modem* Telkom IndiHome diset dengan mode *Router*, dimana koneksi ke *Server* Telkom dilakukan *via Point-to-Point Protocol over Ethernet* (PPPoE) oleh *Modem* tersebut. Sehingga yang mendapatkan *IP Public* adalah *interface* dari *Modem*. Sedangkan *Router* Mikrotik hanyalah mendapat *IP Private* yang disebarkan oleh *DHCP Server Modem*.

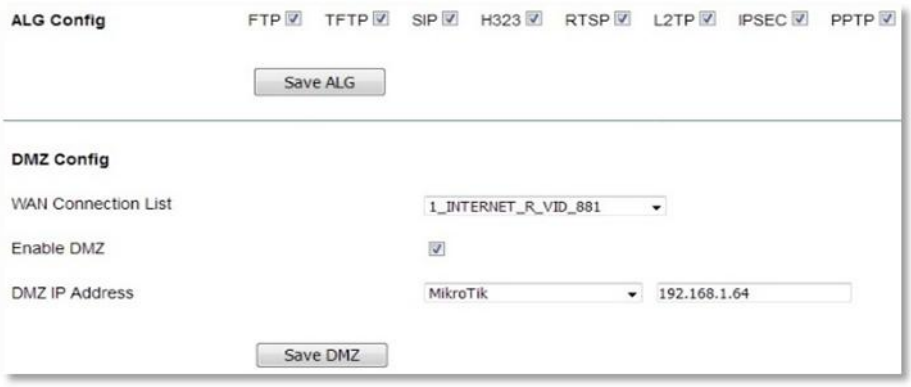
Bisa diketahui bahwa *interface* koneksi *Internet* dari *Router* Mikrotik hanyalah *IP Private*, sehingga Router Mikrotik tersebut tidaklah bisa diakses secara langsung dari *Internet*. Dengan kata lain, *Router* Mikrotik berkomunikasi dengan dunia luar *internet* harus melewati bantuan *filter* NAT dari *Modem*, dan menumpang pada *IP Public* dari *Modem*.

Untuk bisa membuat *Router*, Mikrotik memperoleh *IP Public* pada *interface*-nya, sehingga bisa diakses dari luar, kita bisa memanfaatkan Fitur DMZ pada *Modem* Telkom IndiHome. Sebelum mengaktifkan Fitur DMZ ini, kita perlu melakukan pengaturan pada fungsi *Firewall Modem*. Dimana fungsi *Security Level* dari *firewall* haruslah diset pada *level* "*Low*". Dengan begitu, fungsi DMZ bisa diaktifkan/disupport oleh *Modem*. Gambar 6 memperlihatkan Fungsi *Security Level* pada *firewall*.

Gambar 6. Fungsi *Security Level* pada *Firewall*

Setelah melakukan pengaturan pada *Security Level Firewall*, barulah kita bisa menghidupkan Fungsi/Fitur DMZ. Pada menu pengaturan Fitur DMZ, terdapat beberapa opsi ataupun masukan yang harus kita berikan. Diantaranya *Application Level Gateway* (ALG) *Config*, yang mengatur layanan (*port*) yang akan diteruskan. Dan *DMZ Config*, yang mengatur *interface Internet Modem* yang akan di-*bypass* atau diteruskan ke *Router* Mikrotik, pengaktifan fungsi DMZ, dan *DMZ IP Address*. Untuk *DMZ IP Address* haruslah diisi dengan *IP Private* yang didapat oleh *Router* Mikrotik. Dengan begitu, *Modem* Telkom IndiHome tahu kepada siapa layanan *IP Public* yang dimilikinya akan diteruskan. Gambar 7 akan memperlihatkan *ALG Config* dan *DMZ Config*.

ISBN: 978–623–91277–6–3

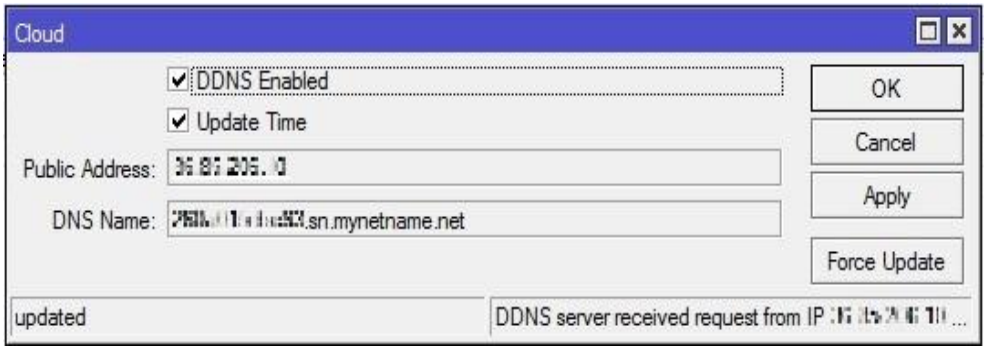


Gambar 7. *ALG Config* dan *DMZ Config*

Setelah melakukan konfigurasi DMZ, *Router* Mikrotik akhirnya bisa memiliki *IP Public* pada *interface*-nya yang terkoneksi ke *internet*. Sehingga *Router* Mikrotik bisa diakses dari *internet* berdasarkan *IP Public* yang telah dimilikinya. Hal yang menjadi kendala berikutnya, walaupun telah mendapatkan *IP Public*, *Router* Mikrotik suatu ketika tidaklah bisa diakses berdasarkan *IP Public* yang telah dicatat sebelumnya. Karena *IP Public* yang dimilikinya bisa berubah-ubah (*Dynamic IP Public*). Hal ini dikarenakan *IP Public* yang didistribusikan dari *server* Telkom ialah *Dynamic IP Public* dan bukanlah *Static IP Public*, untuk setiap pelanggan Telkom IndiHome. Jadi setiap *IP Public* yang sudah kita catat untuk pengaksesan, bisa berubah sendirinya, sehingga tidak bisa diakses lagi.

Untuk mengatasi hal ini, *Router* Mikrotik telah menyediakan fasilitas *IP Cloud*. Dimana setiap *IP Public* yang dimiliki oleh *Router* Mikrotik dikirim ke *server* MikroTik.com untuk dicatat dan diganti dengan sebuah alamat *domain* (*DNS Name*). Sehingga alamat *IP Public* dari *Router* Mikrotik cukuplah diakses melalui sebuah alamat *domain* (*DNS Name*) yang diberikan secara *static*. Jika terjadi perubahan *IP Public*, *Router* Mikrotik akan mengirimkan *IP Public* yang baru tersebut ke *server* MikroTik.com, sehingga *IP Public* yang tersimpan disana tetaplah *uptodate* dan selalu bisa diakses. Untuk tampilan Fitur *IP Cloud* pada *Router* Mikrotik bisa dilihat pada Gambar 8.

Untuk mengaktifkan fitur *IP Cloud*, cukuplah dengan menghidupkan tanda centang pada "*DDNS Enabled*". Selain itu juga, terdapat fitur untuk melakukan sinkronisasi waktu pada *Router* Mikrotik dengan *server* MikroTik.com.

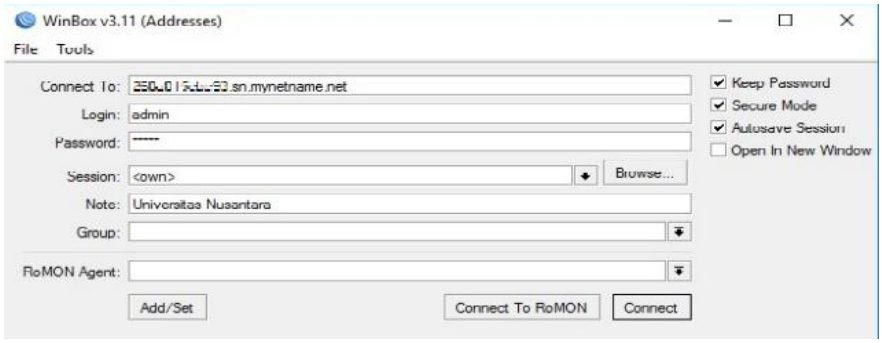


Gambar 8. Fitur *IP Cloud* pada *Router* Mikrotik

ISBN: 978–623–91277–6–3

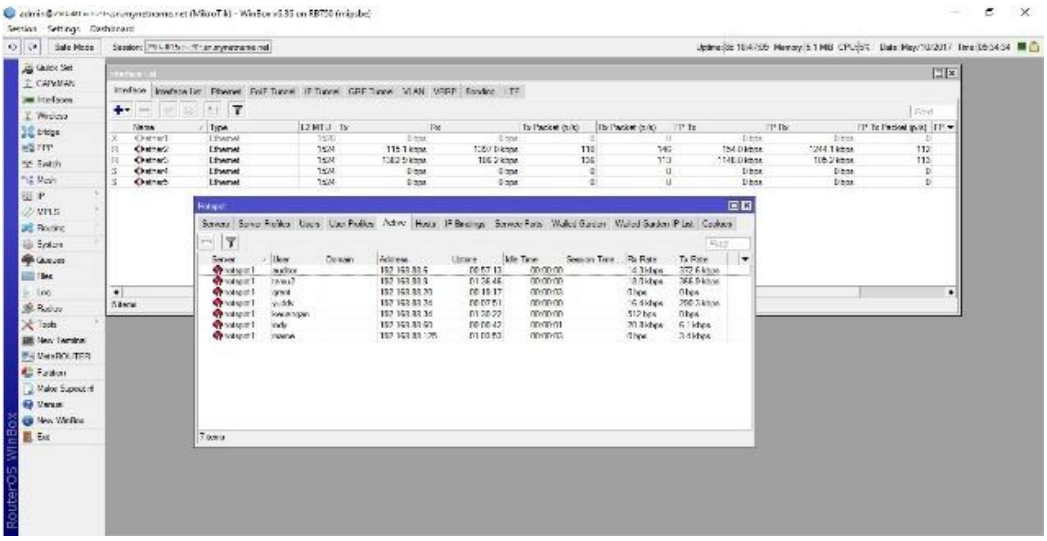
Untuk memastikan bahwa *Router* Mikrotik selalu meng-*update* data *IP Public* yang dimilikinya ke *server* MikroTik.com, kita bisa melakukan proses "*force update*" secara berkala menggunakan fungsi *Script* dan *Schedule* pada *Router* Mikrotik.

Setelah melakukan konfigurasi *IP Cloud*, selanjutnya kita bisa mencoba melakukan pengaksesan terhadap *DNS Name* dari *Router* Mikrotik kita. Untuk memastikan bahwa *DNS Name* dari *Router* Mikrotik kita hidup, *valid*, dan merespon, maka kita terlebih dahulu melakukan proses "*ping*". Setelah memastikan bahwa *DNS Name* dari *Router* Mikrotik kita bisa diakses lewat *ping*. Selanjutnya kita akan mencoba pengaksesan terhadap *Router* Mikrotik lewat aplikasi WinBox. Untuk contoh pengaksesan *Router* Mikrotik lewat aplikasi WinBox bisa dilihat pada Gambar 9.



Gambar 9. Contoh Pengaksesan *Router* Mikrotik lewat Aplikasi WinBox

Dari Gambar 9, bisa dilihat bahwa kita cukup memasukkan *DNS Name* dari *Router* Mikrotik kita ke dalam isian "*Connect To*". Dan tidak perlu menghafal ataupun mencatat *IP Public* dari *Router* Mikrotik kita yang terus berubah-ubah. Setelah melakukan proses *Connect*, kita akan terhubung dengan *Router* Mikrotik kita, dan akan tampak tampilan menu utama dari aplikasi WinBox, seperti pada Gambar 10. Lewat tampilan menu utama dari aplikasi WinBox, kita bisa melakukan proses konfigurasi ataupun *monitoring* jaringan yang kita inginkan. Selain menggunakan aplikasi WinBox, kita juga bisa menggunakan aplikasi *android* untuk mengakses *Router* Mikrotik kita. Misalnya dengan aplikasi Mikro Winbox ataupun Tik-App.



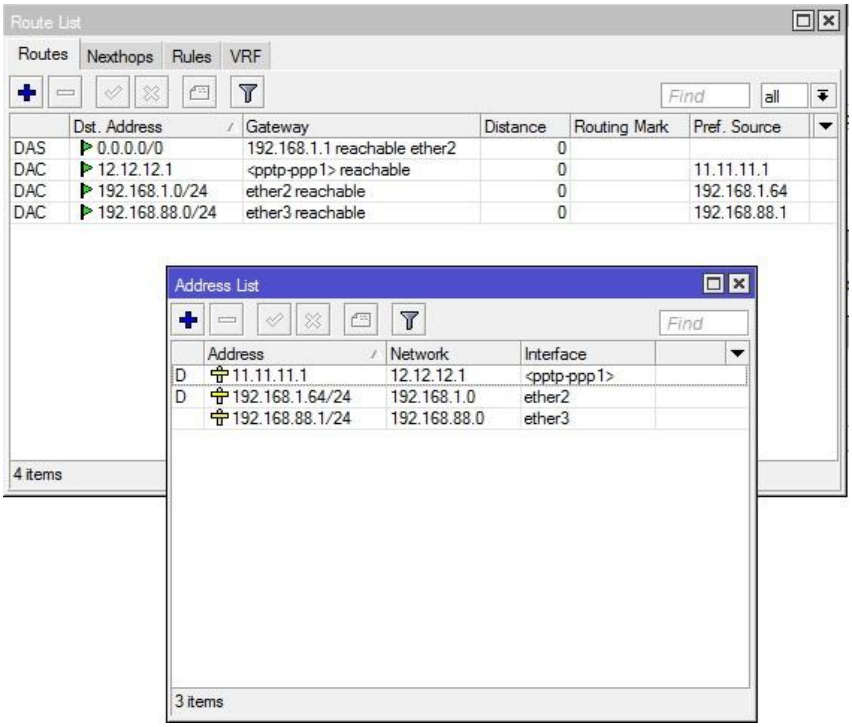
Gambar 10. Tampilan Menu Utama dari Aplikasi WinBox

ISBN: 978–623–91277–6–3

Selain untuk pengontrolan jarak jauh *Router* Mikrotik, fitur *IP Cloud* dan DMZ bisa digunakan untuk membantu proses koneksi *Virtual Private Network* (VPN). Dimana *server* VPN, misalnya menggunakan *Point-to-Point Tunneling Protocol* (PPTP) tidak perlu membutuhkan adanya *IP Public* yang *static* untuk *interface* koneksinya. Melainkan hanya membutuhkan *DNS Name* dari *IP Cloud* untuk membangun koneksi. Seperti kita tahu bahwa untuk berlangganan suatu *IP Public* yang *static* akan memakan biaya yang lebih banyak dibandingkan dengan *IP Public* yang *dynamic*. Oleh karena itu, dengan menggunakan teknik/metode ini kita bisa menghemat dana untuk pembelian *IP Public Static*.

Untuk melakukan koneksi PPTP, terlebih dahulu kita harus melakukan pengaturan pada *Router* Mikrotik untuk mengaktifkan fasilitas ini. Setelah aktif barulah kita bisa mencoba melakukan koneksi ke *PPTP Server* yang telah dibuat tersebut. Untuk mengkoneksikan ke *PPTP Server*, kita bisa menggunakan *Personal Computer* (PC), baik *laptop* maupun *desktop*. Sebagai contoh, kita menggunakan komputer *desktop* dengan sistem operasi Windows 10. Sebagai komputer *Client*, kita perlu memasukkan data *PPTP Client* agar bisa terkoneksi ke *PPTP Server* pada *Router* Mikrotik. Disini kita hanya perlu memasukkan *Server Name* atau *DNS Name* tanpa perlu suatu *IP Public Static*. Setelah terkoneksi ke *PPTP Server*, kita bisa melakukan aktifitas layaknya sedang berada dalam lingkup LAN dengan *Router* Mikrotik. *Router* Mikrotik bisa diakses oleh aplikasi WinBox, hanya dengan menggunakan IP Lokalnya, misalnya 192.168.88.1.

Fungsi lainnya ketika kita terkoneksi ke suatu *VPN Server* (*PPTP Server*), kita bisa mengakses semua komputer/*device* lokal (IP Lokal) yang terhubung secara langsung ke *interface*-nya *Router* Mikrotik. Untuk bisa melihat daftar IP Lokal yang dipasang ke *interface Router* Mikrotik bisa dilihat pada Gambar 11.

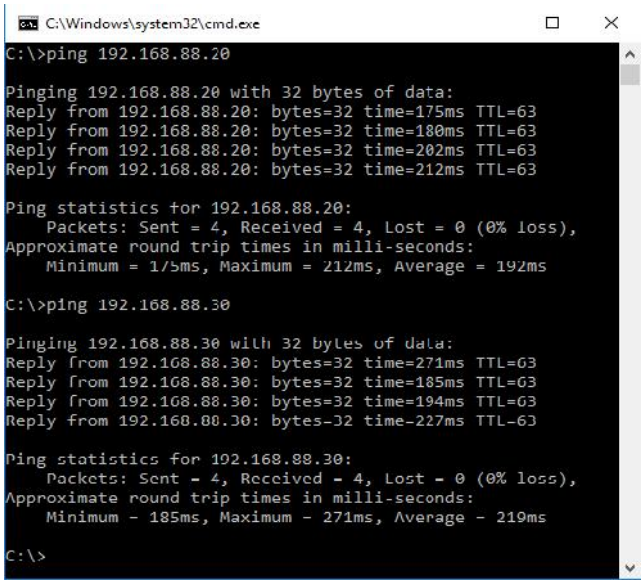


Gambar 11. Daftar IP Lokal yang dipasang ke *Interface Router* Mikrotik

ISBN: 978–623–91277–6–3

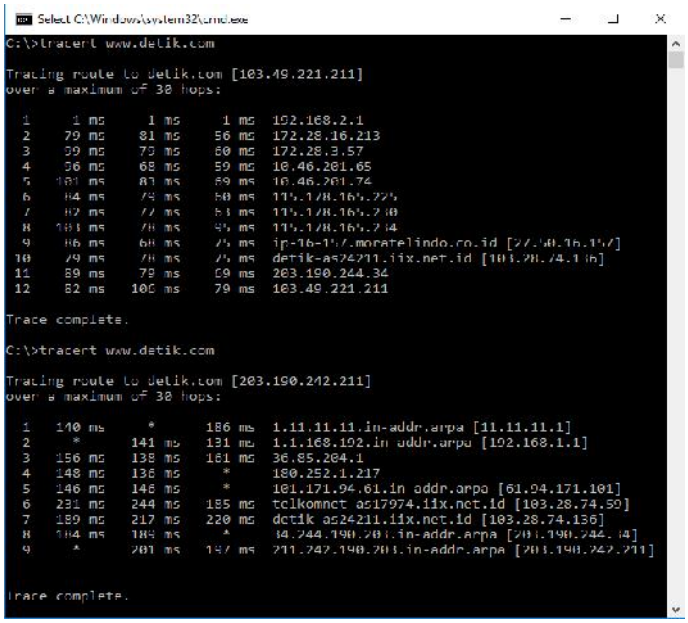
Sebagai contoh, kita bisa mengakses *Modem* Telkom IndiHome yang terkoneksi ke *interface*-nya *Router* Mikrotik, dengan IP Lokal 192.168.1.1 pada ether2. Dan semua itu bisa kita lakukan dari luar melalui jaringan *Internet*. Tanpa terhalangi oleh *IP Public* dan *filter* NAT yang ada.

Selain itu juga, kita bisa mengakses semua komputer/*device* lokal lainnya yang ada, misalnya yang terkoneksi ke ether3, dengan IP Lokal 192.168.88.1/24. Gambar 12 memperlihatkan pengaksesan komputer lokal lainnya lewat uji *ping*.



Gambar 12. Pengaksesan Komputer Lokal lainnya lewat Uji *Ping*

Semua komputer/*device* lokal bisa kita akses, sekaligus komputer/*device* lokal bisa mengakses komputer kita. Hal ini bisa terjadi dikarenakan proses *routing* yang telah dilakukan dengan benar, seperti pada Gambar 11. Sebagai akhir dari pembahasan, akan diperlihatkan perbandingan antara jalur/rute pengaksesan tanpa VPN dan dengan VPN, seperti pada Gambar 13.



Gambar 13. Perbandingan antara Jalur/Rute Pengaksesan Tanpa VPN dan dengan VPN

ISBN: 978–623–91277–6–3

Dari Gambar 13 bisa dilihat bahwa ketika kita menggunakan VPN, maka rute pengaksesan kita akan melalui *server* VPN (11.11.11.1 => *Router* Mikrotik dan 192.168.1.1 => *Modem* Telkom IndiHome). Dan ketika tanpa VPN, maka rute pengaksesan kita akan melalui rute *default* dari *Internet Provider* yang sedang kita gunakan. Rute yang digunakan akan berbeda-beda meskipun tujuan (*destination*) pengaksesan adalah sama.

4. KESIMPULAN

Implementasi *IP Cloud* dan DMZ telah berhasil dilakukan guna mendukung proses pengendalian jarak jauh *Router* Mikrotik. Masalah *Dynamic IP Public* dan *filter* NAT telah bisa diatasi dengan kedua fitur ini. Selain untuk pengaksesan jarak jauh *Router* Mikrotik, fitur *IP Cloud* dan DMZ ini juga sangat membantu dalam proses pembuatan *server* VPN, misalnya *PPTP Server*. Sehingga *PPTP Server* bisa diakses oleh *PPTP Client* hanya dengan menggunakan *Server Name* atau *DNS Name*.

Saran

Hasil penelitian yang dibahas di sini hanyalah contoh kecil dari pemanfaatan fitur *IP Cloud* dan DMZ. Sehingga ke depannya diharapkan bisa diimplementasikan ke berbagai contoh penggunaan lainnya. Misalnya untuk pengaksesan *web server* lokal ataupun pengaksesan *file server/database* lokal, yang melalui *Internet*. Tentunya semuanya ini dilakukan dengan memanfaatkan bantuan fitur *IP Cloud* dan DMZ.

Penghargaan/Ucapan Terima Kasih

Penulis/peneliti mengucapkan terima kasih kepada Rektor Universitas Nusantara Manado dan Ketua Yayasan Universitas Nusantara Manado, yang telah memberi *support* dan fasilitas untuk melakukan penelitian dan pengembangan di Laboratorium/*Server* ICT Universitas Nusantara Manado.

DAFTAR PUSTAKA

Hariono, H. A. Memahami *Firewall* DMZ. Diakses dari http://www.jaringan-komputer.cv-sysneta.com/memahami-firewall-dmz, tanggal 4 Mei 2017.

Citraweb Nusa Infomedia. Solusi *Dynamic IP Public* dengan *IP Cloud*. Diakses dari http://www.mikrotik.co.id/artikel_lihat.php?id=89, tanggal 6 Mei 2017.