Jurnal KomtekInfo

https://jkomtekinfo.org/ojs

2021 Vol. 8 No. 3 Hal: 169-175 p-ISSN: 2356-0010, e-ISSN: 2502-8758

Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan

Prayogi Wicaksana[1]✉, Febri Hadi[2], Aulia Fitrul Hadi[3]
Universitas Putra Indonesia YPTK Padang, Indonesia

wicaksana.prayogi@gmail.com

Abstract

One of the ways to maintain and improve the quality of service and security on the network of an agency of the Barangin Sub-District Office, Sawahlunto City (Central) is to add a VPN feature. Administrators who always monitor the flow of traffic by accessing routers and access points to find out network conditions. There are times when the Administrator is on a public network, he or she cannot access routers and access point devices because the Public IP obtained is Dynamic (random). To solve this problem, it is done through the Network Development Life Cycle (NDLC) method by combining the L2TP and IPsec VPN protocol systems on Mikrotik. A Virtual Private Network (VPN) is a private and secure network using a public network such as the internet. One of the bases for securing VPN technology is Internet Protocol Security (IPSec). IPSec is a protocol used to secure datagram transmission on TCP/IP-based networks. This study aims to design and implement a VPN network system by utilizing a public network, where this system provides advanced security enhancements on the internet network using IPSec. The information/data sent will be confidential with an automatic encryption method through the L2TP tunnel method from the server to the branch/client computer and vice versa. The VPN is implemented using a layer 2 (L2TP) tunneling protocol using two Mikrotik routers. There are few changes to the computer network configuration to minimize costs and implementation time. Tests are carried out to implement security on the network using the command prompt, where the admin observes packet loss and delay parameters to determine the increase in security quality on the network.

Keywords: Virtual Private Network (VPN), Mikrotik, Protokol Tunneling Layer 2 (L2TP), IPsec, Network Development Life Cycle (NDLC).

Abstrak

Salah satu cara yang dilakukan untuk menjaga dan meningkatkan kualitas layanan dan keamanan pada jaringan suatu instansi Kantor Camat Barangin Kota Sawahlunto (Pusat) adalah dengan menambahkan fitur VPN. Administrator yang selalu memonitoring jalannya lalu lintas dengan mengakses router dan *access point* untuk mengetahui kondisi jaringan. Ada kalanya ketika Administrator berada pada jaringan publik maka tidak dapat mengakses router dan perangkat *access point* dikarenakan IP Publik yang didapatkan bersifat Dynamic (acak). Untuk mengatasi permasalah tersebut dilakukan dmelalui metode *Network Development Life Cycle* (NDLC) dengan mengabungkan sistem protokol VPN L2TP dan IPsec yang ada pada mikrotik. VPN merupakan sebuah jaringan *private* dan aman dengan menggunakan jaringan publik seperti internet. Salah satu basis pengamanan teknologi VPN adalah *Internet Protocol Security* (IPSec). IPSec merupakan protokol yang digunakan untuk mengamankan transmisi datagram pada jaringan berbasis TCP/IP. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem jaringan *Virtual Private Network* (VPN) dengan memanfaatkan jaringan publik, dimana sistem ini memberikan peningkatan keamanan tahap lanjut pada jaringan internet dengan menggunakan IPSec. Informasi/data yang dikirimkan akan bersifat rahasia dengan metode enkripsi otomatis melalui metode tunnel L2TP dari server ke komputer cabang/klien dan sebaliknya. VPN diimplementasikan menggunakan Protokol Tunneling Layer 2 (L2TP) menggunakan dua router Mikrotik. Hanya ada sedikit perubahan pada konfigurasi jaringan komputer untuk meminimalkan biaya dan waktu implementasi. Pengujian dilakukan untuk mengimplementasikan keamanan pada jaringan menggunakan *command prompt*, dimana admin mengamati parameter packet loss dan delay untuk mengetahui peningkatan kualitas keamanan pada jaringan.

Kata kunci: Virtual Private Network (VPN), Mikrotik, Protokol Tunneling Layer 2 (L2TP), IPsec, Network Development Life Cycle (NDLC).

1. Pendahuluan

Instansi Kantor Camat Barangin Kota Sawahlunto merupakan kantor yang berperan penting dalam mengalokasikan data masyarakat guna untuk mengidentifikasikan bahwa masyarakat tersebut merupakan asli penduduk sekitar dengan mendaftarkan diri sebagai penduduk angota setempat, sehingga dapat menunjukan Kartu Keluarga (KK) dan Kartu Tanda

Diterima: 06-08-2021 | Revisi:14-08-2021 | Diterbitkan: 30-09-2021 | DOI: 10.35134/komtekinfo.v8i3.128

Penduduk (KTP). Saat ini teknologi jaringan komputer yang digunakan masih pada jaringan Local Area Network (LAN) dalam pelaksanaan kegiatan operasional kerja setiap hari dan *Mikrotik Routerborad* untuk mengatur arus lalulintas pengguna di internet.

Seiring dengan penggunaan data komunikasi dan informasi yang sangat tinggi, menimbulkan beberapa persoalan dalam keamanan jaringan.

Pengembangan sistem merupakan upaya persiapan sistem baru untuk menggantikan sistem yang sudah ada[1]. Metode yang digunakan dalam pengembangan sistem ini dengan *Network Development Life Cycle* (NDLC) yang merupakan metode yang bergantung pada proses perancangan dan pengembangan jaringan bisnis yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan mekanisme jaringan sehingga top- pendekatan ke bawah dapat dilakukan [2].

Jaringan adalah interkoneksi dari sekumpulan perangkat yang mampu berkomunikasi [3]. Sedangkan internet merupakan adalah kependekan dari jaringan interkoneksi dengan jangkauan jaringan komputer yang lebih luas dari Wide Area Network (WAN) [4]. Jaringan Virtual Private Network (VPN) merupakan salah satu cara untuk mencegah dan melindungi pertukaran data informasi melalui jaringan internet [5]. VPN merupakan koneksi virtual yang bersifat private, dinamakan demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual menghubungkan komputer dengan jaringan publik secara *private* [6].

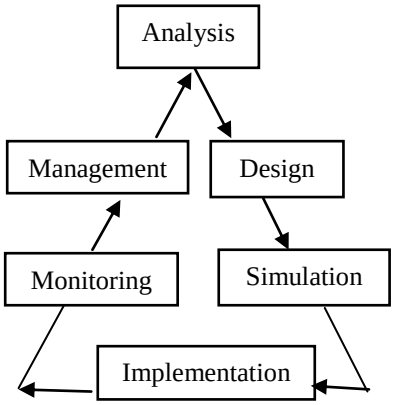
Keamanan VPN terdiri dari beberapa komponen, yaitu otentikasi user, merupakan proses dalam rangka validasi user saat memasuki sistem [7]; kontrol akses, adalah mekanisme yang digunakan untuk mengamankan dan menentukan kerahasiaan informasi [8]; enkripsi, adalah proses pengubahan, penyandian atau penyandian suatu pesan (informasi) [9]; public key infrastructure (PKI). Infrastruktur keamanan yang dijalankan dengan menggunakan konsep dan teknik kriptografi kunci publik [10]. Didalam VPN terdapat berupa *tunnel* yang merupakan podasi dasar dari sebuah sistem VPN yang bertugas untuk membangun, menangani dan menyediakan koneksi point-to-point dari sumber ke tujuan[11]. Terdapat tiga protokol pendukung proses pada *tunneling* yang terdiri dari carrier protocol, protokol yang digunakan oleh jaringan tempat informasi berjalan di atasnya seperti Transmission Control Protocol/User Datagram Protocol (TCP/UDP); encapsulating protocol, protokol ini membungkam data asli di dalamnya seperti seperti IPSec, L2TP; Passanger Protocol, protokol yang menerima data asli dari server seperti Internet Protocol (IP) [12].

Point to Point Tunneling Protocol (PPTP) adalah protokol jaringan yang memungkinkan transfer data aman melalui TCP/IP [13]. Sedangkan L2TP adalah pengembangan dari PPTP plus L2F. Protokol Tunneling Layer 2 (L2TP) juga sering disebut sebagai protokol dial-up virtual, karena L2TP memperluas sesi dial-up Point to Point Protocol (PPP) melalui jaringan internet public dan memiliki tingkat keamanan yang lebih tinggi dibandingkan PPTP yang hanya menggunakan MPPE [14]. IPSec merupakan protokol yang digunakan untuk mengamankan transmisi datagram pada jaringan berbasis TCP/IP. IPSec menawarkan 3 layanan utama, yaitu otentikasi dan integritas data, kerahasiaan, dan manajemen kunci [15]. Untuk dapat memenuhi kebutuhan keamanan L2TP perlu dicoba implementasi keamanan dengan menggunakan protokol tipe transport IPSec atau lebih dikenal dengan protokol L2TP over IP Security (IPSec), sehingga paket informasi yang dikirim oleh protokol L2TP akan terenkapsulasi oleh protokol IPSec [16]. Mikrotik RouterOS merupakan salah satu pendukung dalam penkonfigurasian VPN dimana sistem operasi yang dipakai berbasis linux yang khusus digubakan untuk peran Sistem Perutean [17].

Penelitian dilakukan atas kesadaran pemahaman yang terbatas yang didapat pada jurnal-jurnal sebelumnya, guna untuk mengembangkan metode yang digunakan sebelumnya dan dorongan keingintahuan atas segala masalah sehingga dapat merancang suatu solusi yang lebih baik, efektif, efisien dan terjangkau dari hal *network security*. Penelitian memberikan rumusan masalah yang dimana nantinya peneliti akan merancang jaringan vpn *server* dengan metodi L2TP dan IPSec guna meningkatkan ketahanan pada sistem jaringan agar diharapkan dapat memberikan alternatif solusi pada keamanan jaringan tersebut.

2. Metodologi Penelitian

Penelitian akan menerapkan pengembangan sistem dengan menggunakan metode Network Development Life Cycle (NDLC). Adapun tahapan dalam menggunakan metode NDLC terdiri dari: Analysis, Design, Simulasi, Implementasi, Monitoring, Management [18]. Adapun penelitian ini dapat di jelaskan pada tahapan penelitian yang terdapat pada Gambar 1.



Gambar 1 *Network Development Life Cycle* (NDLC).

Gambar.1 menjelaskan tahapan yang dilakukan dalam penelitian. Metode NDLC akan terfokus pada tahapan analis, design, simulasi, dan implementasi. Metode penelitian yang dilakukan adalah sebagai berikut:

a. Penelitian Lapangan

Penelitian ini dilakukan dengan mewawancarai staf yang bekerja di departemen TI khususnya, mengajukan pertanyaan dan menganalisis masalah serta memperoleh data yang diperlukan.

b. Perpustakaan Penelitian (Library Research)

Penelitian kepustakaan ini dilakukan dengan cara membaca jurnal, buku, internet, artikel yang membahas tentang jaringan komputer, VPN Server, L2TP, PPTP, IPSec dan yang berkaitan dengan Keamanan Jaringan. Sehingga data yang diperoleh dapat digunakan sebagai dasar untuk tahap penelitian selanjutnya.

2.1 Analisis

Berdasarkan identifikasi masalah di atas, peneliti melakukan analisis data terlebih dahulu. Hal ini agar pemecahan masalah dapat menghasilkan solusi baru.

2.2 Perencanaan sistem

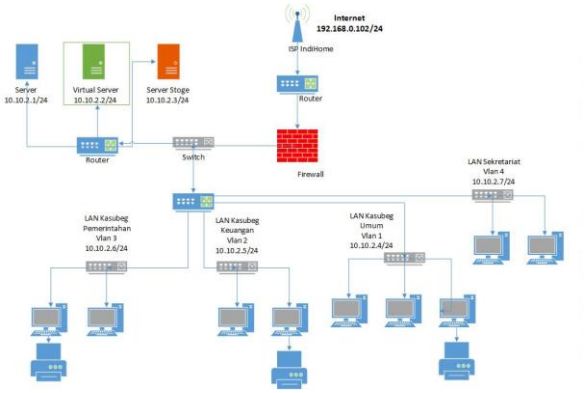
Pada tahap perancangan topologi jaringan dengan metode L2TP dan IPSec sebagai keamanan jaringan menggunakan aplikasi Cisco packet tracer sebagai replika dari sistem yang akan dijalankan.

2.3 Implementasi Sistem

Sesi pengujian ini dilakukan untuk mengetahui apakah simulasi jaringan dapat berjalan dengan sukses tanpa kesalahan dengan perencanaan awal. Pengujian dicoba hanya pada satu komputer server dan beberapa komputer klien dengan tujuan untuk mengidentifikasi apakah desain sesuai dengan rencana awal. Pengujian server VPN dicoba dengan menguji konektivitas paket informasi request reply ke jaringan internet melalui fitur proxy.

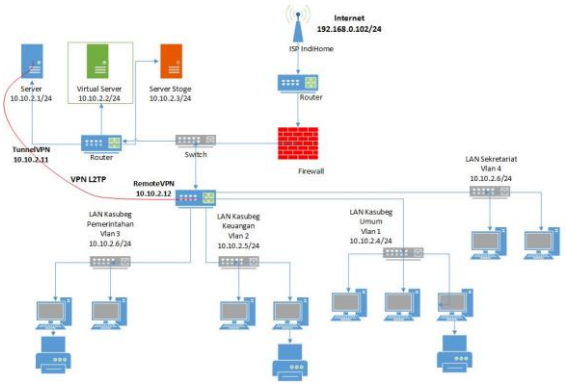
3. Hasil dan Pembahasan

Perbandingan antara skema topologi sebelum dan sesudah di tambahkan fitur VPN pada jaringan LAN Kantor Camat Barangin Kota Sawahlunto. Adapun topologi yang digunakan dapat dilihat pada Gambar 2.



Gambar 2. Skema Topologi LAN

Topologi jaringan star yang digunakan pada instansi Kantor Camat Barangin yang belum menggunakan pembentukan dari VPN terdapat pada Gambar 3.



Gambar 3. Skema Topologi Jaringan VPN L2TP

Topologi usulan jaringan star yang pada instansi Kantor Camat Barangin yang telah menggunakan bentukan dari VPN. Dalam mengusulkan topologi jaringan yang akan diimplementasikan tidak akan merubah bentuk topologi yang ada, karena bentuk topologi yang digunakan sudah sangat baik. Topologi yang digunakan adalah topologi star. Dan disarankan untuk menggunakan VPN untuk berkomunikasi atau bertukar data pribadi agar lebih aman.

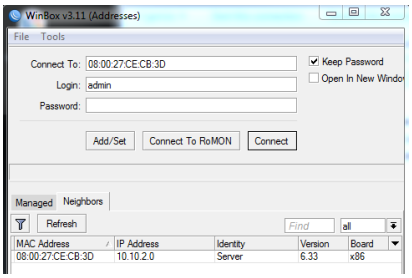
Dalam perancangan jaringan VPN L2TP ada beberapa langkah yang harus dilakukan, sistem yang sesuai dengan perancangan akan memudahkan dalam mengelola konfigurasi jaringan dan tidak membuat seorang administrator tidak bingung dalam mengelolanya.

3.1 Desain Jaringan

Pada perancangan sistem jaringan berikut ini peneliti akan membuat jaringan VPN dengan metode L2TP/IPsec untuk menghubungkan komputer server dengan komputer client/cabang di kantor Camat. Berikut adalah tahapan konfigurasi pada server sisi router (CHR).

3.1.1. Winbox merupakan aplikasi portable yang bisa digunakan tanpa harus menginstal terlebih dahulu.

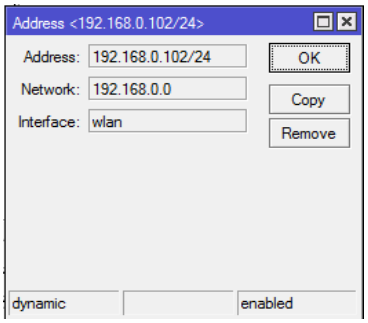
Konfigurasi ke Mikrotik menggunakan software Winbox disajikan pada Gambar 4.



Gambar 4. Tampilan Winbox

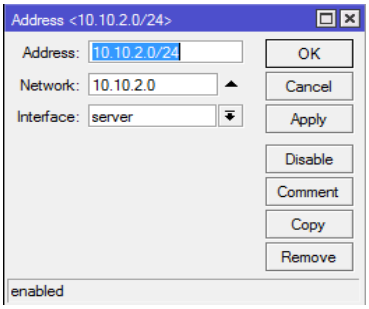
Aktifkan winbox untuk konek ke internet dengan mengklik *Connect To* tunggu hingga muncul alamat MAC Address setelah mucul, klik login dengan konfigurasi *default* yang tertera pada aplikasi dan *Connect.*

3.1.2. Konfigurasi Alamat IP



Gambar 5. Konfigurasi IP wlan

Gambar 5 merupakan Either 1 merupakan port pertama yang digunakan untuk mengkonfigurasi IP wlan yang berfungsi *gatway* sebagai penghubung ke internet.

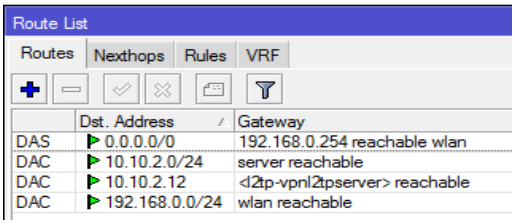


Gambar 6. Konfigurasi IP lokal

Gambar 6 merupakan Either 2 merupakan port kedua yang digunakan untuk mengkonfigurasi IP lokal yang berfungsi sebagai *gatway* untuk penghubung ke PC.

3.1.3. Konfigurasi Router

Konfigurasi NAT di firewall. NAT merupakan pemetaan alamat IP sehingga banyak IP private dalam sebuah LAN dapat mengakses IP publik. Setelah menginstal Mikrotik, langkah selanjutnya adalah mengkonfigurasi NAT melalui terminal. Setelah membentuk konfigurasi server untuk dapat terkoneksi dengan internet, langkah selanjutnya adalah membuat konfigurasi proxy untuk membuat teknologi VPN yang disajikan pada Gambar 7.

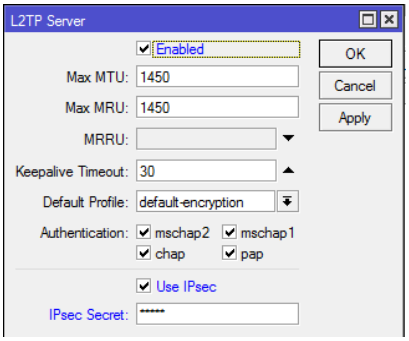


Gambar 7. Konfigurasi Router

Konfigurasi router dengan menambahan IP tunnel VPN berfungsi sebagai penghubung antara server dengan cabang/client.

3.1.4. Konfigurasi Server L2TP

Pemilihan menu pertama adalah memilih menu PPP di sisi kiri winbox hingga muncul kotak dialog PPP. Pada kotak dialog PPP, pilih menu server L2TP hingga muncul kotak dialog server L2TP yang disajikan pada Gambar 8.

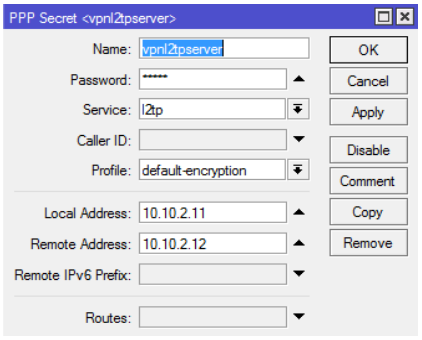


Gambar 8. Konfigurasi Server L2TP

Pada kotak form L2TP Server isi dengan mencantang *enable*, untuk *default profile* pilih *default-encryption* dan IPSec Secret masukan katasandi yang diinginkan.

3.1.5. Konfigurasi Secret L2TP

Pada bagian ini, tujuan dari pembuatan rahasia L2TP adalah untuk membuat akun bagi pengguna yang akan mengakses jaringan VPN yang disajikan pada Gambar 9.

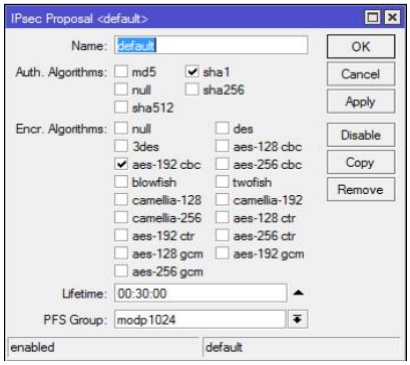


Gambar 9. Konfigurasi Secret L2TP

Pada *form* PPP Secret diisi sesuai kebutuhan id yang akan digunakan unutk mengubung antar jaringan VPN server dengan client.

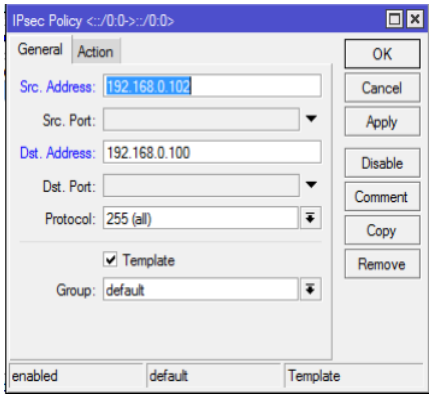
3.1.6. Konfigurasi IPSec

Enskripsi pada L2TP/IPSec memiliki tingkat sekuritas lebih baik dan tinggi daripada PPTP yang menggunakan MPPE yang disajikan pada Gambar 10.



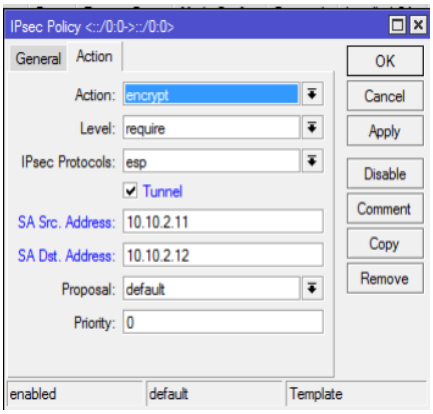
Gambar 10. Konfigurasi IPSec Protocol

Pada form yang tersedia pilih *default.* Klik Oke. Lanjut ke menu form selanjutnya dengan menambahkan IPSec Policy yang disajikan pada Gambar 11.



Gambar 11. Konfigurasi IPSec Policy

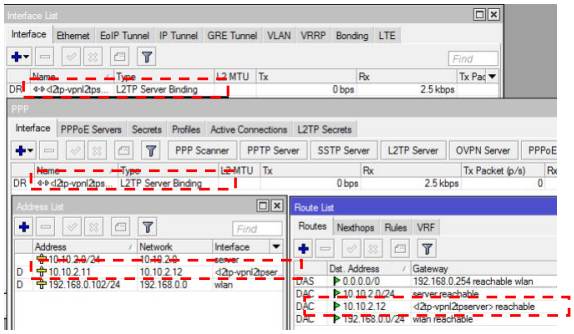
Pada menu IPSec Policy pilih form General maka akan muncul Src. Address yang dimana merupakan IP wlan server dan Dst. Address merupakan IP Client. Lanjut ke form sebelahnya dengan mengklik Action yang disajikan pada Gambar 12.



Gambar 12. Konfigurasi New IPSec Policy

Pada form Action, centang *Tunnel* dan isi alamat address VPN yang telah dibuat pada server, dan klik Ok.

3.1.7. Hasil dari Konfigurasi L2TP Server dan IPSec



Gambar 13. Konfigurasi New IPSec Policy

Hasil konfigurasi pada Gamabr 13 secara otomatis membentuk rule VPN pada router sendiri, menujukan bahwa hasil konfigurasi berhasil.

3.1.8. Konfigurasi klien/cabang VPN

Langkah awal pembuatan VPN client menggunakan fasilitas yang beredar di windows 7 yaitu Network dan sharing center, kemudian dilanjutkan dengan proses koneksi VPN, kemudian terbentuklah VPN pada remote client yang disajikan pada Gambar 14.

Gambar 14. Pembuatan Rahasia L2TP

Pada form ini, gunakan akun yang telah dibuat pada router server sebelumnya guna untk terubung satu *(server)* dengan yang lain *(client).*

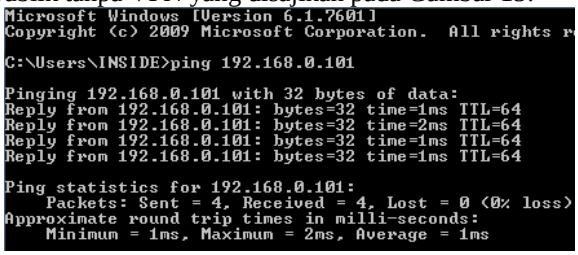
3.1.9. Pengujian Jaringan

Dalam hal pengujian jaringan ada 2 cara untuk mendapatkan hasil yang maksimal. Khususnya dalam merancang teknologi VPN, yaitu:

3.1.9.1. Pengujian jaringan awal

a. *Packet Loss Test*

Pengujian packet loss dilakukan beberapa kali dengan perintah "ping" ke IP tujuan menggunakan command prompt untuk melihat kestabilan koneksi pada jaringan publik tanpa VPN yang disajikan pada Gambar 15.

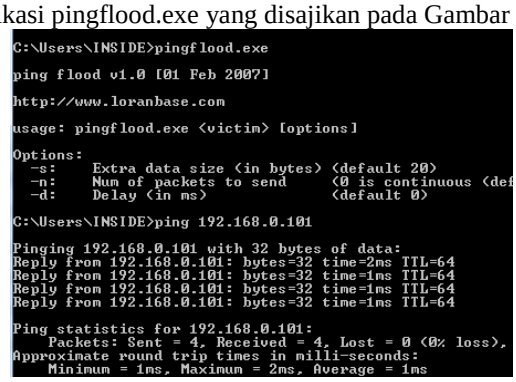


Gambar 15. Packet loss Jaringan awal

Dan hasilnya adalah untuk data max dan rata-rata pulang pergi sebuah paket masih dalam batas wajar. Dari percobaan 4 paket, max round trip = 2ms dan rata-rata round trip = 1ms.

b. *Daniel of Services Test*

Tes ini berguna untuk melihat resistansi koneksi saat dalam serangan ddos. Pengujian dilakukan dengan aplikasi pingflood.exe yang disajikan pada Gambar 16.



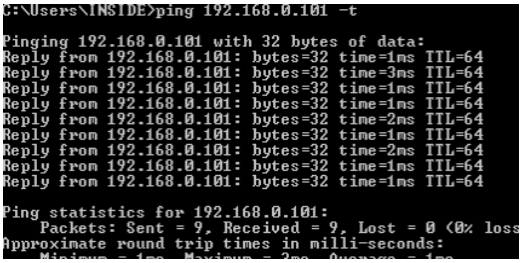
Gambar 16. Serangan DoS Jaringan awal

Setelah dilakukan pengujian dengan mengirimkan 4 paket data sebesar 25 kb, didapatkan hasil bahwa jaringan tidak terputus dan maksimum round trip adalah 2ms.

3.1.9.2. Tes jaringan akhir

a. *Packet Loss Test*

Pengujian packet loss dilakukan beberapa kali dengan perintah "ping" ke IP tujuan menggunakan command prompt untuk melihat kestabilan koneksi pada jaringan publik menggunakan L2TP/IPSec VPN yang disajikan pada Gambar 17.

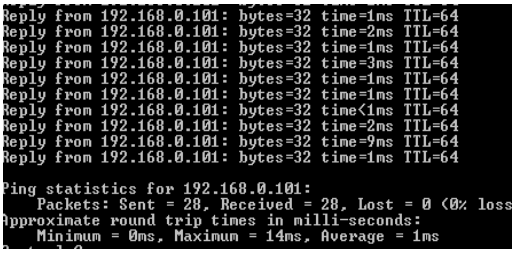


Gambar 17. Jaringan akhir packet loss

Dan hasilnya adalah untuk data max dan rata-rata pulang pergi sebuah paket masih dalam batas wajar. Dari percobaan 9 paket, max round trip = 3ms dan rata-rata round trip = 1ms.

b. Daniel of Services Test

Tes ini berguna untuk melihat resistansi koneksi saat dalam serangan ddos. Pengujian dilakukan dengan aplikasi pingflood.exe yang disajikan pada Gambar 18.



Gambar 18. Jaringan akhir serangan DoS

Setelah selesaipengujian dengan membanjiri server VPN dengan 28 paket data 25kb. Data yang diperoleh untuk perjalanan pulang pergi maks dan rata-rata suatu paket masih dalam batas wajar.

3.2. Hasil Analisis dan Eksperimen

Setelah merancang perangkat jaringan VPN di kantor Camat menggunakan router Mikrotik untuk mengirim informasi/data rahasia, maka diperoleh hasil sebagai berikut:

a. Server jaringan kantor kecamatan dengan jaringan kantor kecamatan cabang dapat dihubungkan dengan jalur tunneling yang menggunakan jaringan internet.

b. Proses pertukaran data rahasia tidak lagi ditarik secara manual atau menggunakan email, melainkan menggunakan jaringan VPN yang terintegrasi ke dalam jaringan lokal antara kantor pusat dan kantor cabang.

c. Sistem jaringan VPN jauh lebih aman dan dana yang dibutuhkan untuk membangun jaringan VPN dengan router proxy jauh lebih terjangkau.

4. Kesimpulan

Setelah menyelesaikan tahapan pelaksanaan kegiatan dari analisis kebutuhan mulai dari perancangan hingga pengujian dan pembahasan hasil, maka dapat diambil kesimpulan bahwa Perancangan simulasi menggunakan aplikasi Microsoft Visio 2013 dapat dilakukan secara virtual sebagai bentuk blue print sebelum penerapan sistem jaringan diperbaiki. Peningkatan sistem keamanan jaringan dengan mengaktifkan fitur IPSec yang terdapat pada router sehingga proses arus balik informasi terjamin kerahasiaan dan keamanannya. IPSec juga dapat digabungkan dengan sistem keamanan lain seperti proxy dan firewall, untuk menerapkan keamanan berlapis pada jaringan atau disebut juga keamanan berlapis ganda. Dengan menggunakan

jaringan VPN Server dengan metode L2TP/IPSec maka keamanan sistem jaringan akan meningkat karena supporter IPSec yang melakukan enkripsi otomatis terhadap informasi yang dikirimkan pada jaringan. Implementasi jaringan server VPN dengan metode L2TP/IPSec terbilang mudah dan dapat dilakukan dengan mudah sehingga tidak memerlukan keahlian khusus yang harus dimiliki oleh administrator jaringan.

Daftar Rujukan

[1] Pambudi, R., & Muslim, M. A. (2017). Implementasi Policy Base Routing dan Failover Menggunakan Router Mikrotik untuk Membagi Jalur Akses Internet di FMIPA Unnes. *Jurnal Teknologi Dan Sistem Komputer*, *5*(2), 57. doi:10.14710/jtsiskom.5.2.2017.57-61

[2] Doni, F. R. (2019). Implementasi Manajemen Bandwidth pada Jaringan Komputer dengan Router Mikrotik. *EVOLUSI : Jurnal Sains dan Manajemen*, *7*(2). doi:10.31294/evolusi.v7i2.5843.

[3] Setiawan, B., Suryanita, R., & Djauhari, Z. (2017). Prediksi Tingkat Kinerja Struktur Gedung Kantor Berdasarkan Mutu Beton dengan Metode Jaringan Saraf Tiruan. SIKLUS: Jurnal Teknik Sipil, 3(2), 107–116. doi:10.31849/siklus.v3i2.393

[4] Siyamto, Y. (2018). Analisis Kualitas Layanan Jaringan WLAN Dengan Metode QoS Pada Taman Internet Kota Batam. Jurnal Teknik Ibnu Sina (JT-IBSI), 3(2). doi:10.36352/jt-ibsi.v3i2.136.

[5] Simpony, B. K. (2021). Simple Queue Untuk Manajemen User dan Bandwidth di Jaringan Hotspot Menggunakan Mikrotik. *Jurnal Informatika*, 8(1), 87–92. doi:10.31294/ji.v8i1.9385

[6] Utomo, M. C. C., Mahmudy, W. F., & Anam, S. (2017). Kombinasi Logika Fuzzy dan Jaringan Syaraf Tiruan untuk Prakiraan Curah Hujan Timeseries di Area Puspo – Jawa Timur. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *4*(3). doi:10.25126/jtiik.201743299

[7] Setiawan, E. B. (2012). Analisa Quality Of Services (QoS) Voice Over Internet Protocol (Voip) dengan Protokol H.323 Dan Session Initial Protocol (SIP). *Komputa : Jurnal Ilmiah Komputer Dan Informatika*, 1(2). doi:10.34010/komputa.v1i2.55.

[8] Amiza, I. D., Lindawati, L., & Soim, S. (2020). Implementasi dan Analisis Quality of Service (QoS) pada OpenMeetings dengan Virtual Private Network (VPN). Jurnal Fokus Elektroda : Energi Listrik, Telekomunikasi, Komputer, Elektronika Dan Kendali), 5(4), 19. doi:10.33772/jfe.v5i4.13325

[9] Rahayu, C., & Hartati, T. (2020). Implementasi Autentikasi Keamanan Dan Manajemen Bandwidth pada Jaringan Internet di SDN 001 Sekupang. doi:10.31219/osf.io/37tdb.

[10] 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. doi:10.30812/matrik.v16i2.7.

[11] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., & Zorn, G. (1999). Point-to-Point Tunneling Protocol (PPTP). doi:10.17487/rfc2637).

[12] Warman, I., & Hanafi, A. (2019). Analisa Perbandingan Kinerja Generic Routing Encapsulation (GRE) Tunnel dengan Point to Point Protocol Over Ethernet (Pppoe) Tunnel Mikrotik Routeros. *Jurnal TeknoIf*, *7*(1), 58. doi:10.21063/jtif.2019.v7.1..

[13] Nadeau, T., & van, H. (Eds.). (2006). MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base. doi:10.17487/rfc4382

[14] Nadeau, T., & van, H. (Eds.). (2006). MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base. doi:10.17487/rfc4382.

[15] Information technology. Security techniques. Network security. (n.d.). doi:10.3403/30192110u.

[16] Trihadi, S., Budianto, F., & Arifin, W. (2008). Perancangan Virtual Private Network Dengan Server Linux pada PT. Dharma Guna Sakti. CommIT (Communication and Information Technology) Journal, 2(1), 25. doi:10.21512/commit.v2i1.488

[17] wandanaaris. (2020). Network Security: Interkoneksi Jaringan dengan L2TP + IPSec. doi:10.31227/osf.io/rnw6a.

[18] Desmira, D., & Wiryadinata, R. (2020). Implementasi Jaringan VPN Berbasis Mikrotik: Studi Kasus pada Kantor Kecamatan Walantaka. *Jurnal Ilmu Komputer Dan Bisnis*, 11(2), 2455–2464. doi:10.47927/jikb.v11i2.8