YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 6 Nomor 4 Edisi November 2021 (36-46)

25

PENCEGAHAN PACKET SNIFFING MENGGUNAKAN METODE VPN TUNNEL UNTUK KEAMANAN JARINGAN KOMPUTER BERBASIS MIKROTIK

Mohammad Noviansyah, Hafdiarsya Saiyar
Fakultas Teknik dan Informatika Universitas Bina Sarana Informatika
(Naskah diterima: 1 September 2021, disetujui: 29 Oktober 2021)

Abstract

With the development of information technology in the modern era and during the COVID-19 pandemic, it requires an adequate and secure computer network. The application of Virtual Private Network (VPN) is used for computer networks that carry out encrypted data transactions between users. Network security must be a top priority in the face of attacks that may occur on a computer network. Some common attacks are Denial of Service (DoS), Spoofing, Sniffing, and so on. This study will apply a VPN Tunnel to prevent Packet Sniffing with the LP2TP/IPSec method. IPSec is used to secure the data packets sent, whereas with IPSec VPN the data transmission process will be more secure without any interference because the data that has been sent has been well encrypted.
Keywords: *Virtual Private Network, Sniffing, Tunneling.*

Abstrak

Perkembangan teknologi informasi pada era modern dan masa pandemi covid-19 ini memerlukan jaringan komputer yang memadai dan terjaga keamanannya. Penerapan Virtual Private Network (VPN) digunakan untuk pada jaringan komputer yang melakukkan transaksi data yang telah dienkripsi antar pengguna. Keamanan jaringan harus dijadikan prioritas utama dalam menghadapi serangan yang mungkin terjadi pada suatu jaringan komputer. Beberapa serangan yang umum terjadi seperti Denial of Service (DoS), Spoofing, Sniffing, dan lain sebagainya. Penelitian ini akan menerapkan VPN Tunnel untuk mencegah Packet Sniffing dengan metode LP2TP/IPSec. Untuk mengamankan paket data yang dikirim digunakan IPSec, sedangkan dengan IPSec VPN proses pengiriman data akan lebih aman tanpa adanya gangguan karena data yang telah dikirim telah dienkripsi dengan baik.
Kata Kunci: *Virtual Private Network, Sniffing, Tunneling.*

I. PENDAHULUAN

Perkembangan yang semakin pesat pada segi teknologi informasi pada masa modern dan pandemi yang terjadi secara global dan di Indonesia khususnya. Teknologi infomasi yang berkembang ini terutama penggunaan media internet menjadikannya suatu kebutuhan yang harus tersedia

dalam kegiatan yang dilakukan masyarakat saat ini.

Penggunaan internet ini yang secara khusus memanfaatkan jaringan komputer yang dapat berupa penggunaan media kabel (*wired*) dan nirkabel (*wireless*). Namun seiring perjalanan waktu, penggunaan jaringan komputer menggunakan media nirkabel (*wireless*) menjadikannya lebih populer dikarenakan menawarkan berbagai kemudahan, kebebasan, mobilitas dan fleksibilitas yang tinggi.

Dengan mengacu pada kelebihan yang diperoleh dari penggunaan jaringan komputer secara nirkabel ini, terdapat berbagai ancaman, gangguan, maupun serangan dari pihak-pihak yang tidak bertanggung jawab dikarenakan penggunaan gelombang radio pada teknologi nirkabel ini.

Keamanan jaringan yang mumpuni seharusnya dapat diterapkan pada jaringan komputer khususnya yang berteknologi nirkabel ini agar dapat terhindar dari ancaman maupun serangan yang dapat terjadi. Salah satu serangan yang dapat terjadi yaitu dengan metode *Packet Sniffing* yaitu proses pengendusan (*sniffing*) paket data pada suatu sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa mempedulikan kepada siapa paket data tersebut dikirimkan.

Salah satu metode yang dapat diterapkan dalam pencegahan *Packet Sniffing* ini adalah dengan menerapkan metode *VPN Tunnel* pada jaringan komputer (Sujadi & Burhanuddin, 2017). Penerapan ini diharapkan dapat mencegah ancaman yang dapat terjadi pada suatu jaringan komputer.

II. KAJIAN TEORI

Menurut (Harun Sujadi & Mutaqin, 2017) Jaringan merupakan kombinasi *hardware, software*, dan pengkabelan (*cabling*), yang secara bersama-sama memungkinkan berbagai peranti komputasi untuk berkomunikasi satu sama lain. Sedangkan jaringan komputer merupakan kumpulan dari sejumlah perangkat berupa komputer, *hub, switch, router*, atau perangkat jaringan lainnya yang terhubung dengan menggunakan media komunikasi tertentu.

"Jaringan komputer merupakan kumpulan dari beberapa komputer dan peralatan penunjang lainnya yang terhubung dalam satu kesatuan dan saling terkoneksi". (Rahadjeng & Puspitasari, 2018)

A. Jenis Jaringan Berdasarkan Media yang Digunakan:

1. Jaringan Kabel (*Wired Network*)

Menurut (Sofana, 2013) Wired Network adalah "jaringan komputer yang menggunakan kabel sebagai media penghantar". Jaringan kabel, seperti namanya jaringan komputer ini dibentuk dengan menggunakan koneksi kabel antar komputer Biasanya, koneksi dari jaringan kabel ini menggunakan port untuk koneksi LAN, dimana kabel LAN akan dicolokkan ke dalam *port LAN Card*, untuk kemudian dikoneksikan ke dalam komputer.

Jaringan kabel sebenarnya baik untuk digunakan, karena tidak dipengaruhi oleh kondisi cuaca danjuga penghalang sinyal, namun cukup rumit dan juga ribet dalam mengatur tata letak perkabelannya.

2. Jaringan Tanpa Kabel (*Wireless*)

Menurut (Asteroid & Hendrian, 2016) *Wireless Network* merupakan "sebuah jaringan lokal yang menggunakan teknologi gelombang radio untuk pertukaran data".

Jaringan tanpa kabel atau wireless merupakan salah satu pengembangan jaringan yang saat ini sudah banyak digunakan oleh user. Sinyal GSM, GPRS, 3G, 4G merupakan contoh nyata dari penggunaan jaringan wireless yang kita gunakan sehari hari.

Jaringan wireless membutuhkan satu buah menara atau tower pengirim sinyal, dan juga penempatan chip penangkap sinyal pada komputer, bisa berupa SIM Card, bisa juga berupa modem dan antena. Karenatanpa menggunakan kabel, maka koneksi jaringan wireless ini:

a. Lebih praktis dalam penggunaannya.
b. Tidak perlu menggunakan instalasi kabel.
c. Memiliki cakupan dan juga jangkauan jaringan yang lebih luas dibandingkan jaringan kabel.

B. *Mikrotik Router OS*

Menurut (Rohim et al., 2016) *Mikrotik OS* adalah "salah satu *Operating Sistem Router* bawaan dari Linux". Mikrotik banyak digunakan dikalangan warnet-warnet dan banyak dikembangkan karena settingnya yang mudah dan instalasinya yang sederhana, sistem keamanan yang ditawarkan dari mikrotik OS ini cukup kuat dan susah untuk ditembus.

C. Keamanan Jaringan

Menurut (Varianto & Badrul, 2015) keamanan jaringan adalah "salah satu aspek penting dalam dunia internet suatu jaringan internal perusahaan membutuhkan keamanan khusus yang dapat menjaga data dimana berfungsi sebagai keamanan jaringan".

1. AntiVirus

Antivirus adalah sebuah program komputer yang dapat mendeteksi, melumpuhkan (mematikan kinerja virus) serta menghapus virus komputer dan program berbahaya lainnya.

a) Fix, yaitu sebuah software yang dapat mendeteksi dan menghapus hanya satu jenis virus.
b) Antidot, yaitu sebuah software yang dapat mendeteksi dan menghapus beberapa jenis virus.
c) Antivirus, yaitu sebuah software yang dapat mendeteksi, melumpuhkan dan menghapus banyak jenis virus, dan umumnya akan langsung aktif ketika komputer dijalankan.

2. Firewall

Arie Iswadi (2012) "Pengertian *firewall* yaitu sebuah sistem atau perangkat keamanan khususnya pada jaringan komputer yang bertugas untuk menjaga lalu lintas data di dalam jaringan komputer berjalan dengan aman, dan dalam waktu bersamaan juga mencegah lalu lintas data yang tidak aman untuk masuk di dalam jaringan komputer". Dalam (Roma Doni, 2014)

Firewall biasanya diimplementasikan pada sebuah gateway atau pintu gerbang pada jaringan komputer, kebanyakan saat ini *firewall* digunakan untuk menutupi celah keamanan antara dua jaringan atau network yang berbeda, sehingga jaringan lokal yang berada di bawah *firewall* bisa terbebas dari serangan-serangan yang tidak diinginkan dan merugikan. (Roma Doni, 2014)

3. Virtual Private Network (VPN)

Virtual Private Network atau biasa disebut VPN adalah Sebuah cara aman untuk mengakses local area network yang berada pada jangkauan tertentu, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi.

Menurut (Supriyono et al., 2013) VPN "VPN merupakan sebuah sambungan komunikasi yang bersifat pribadi dan dilakukan secara virtual".

4. Tunneling

Tunnel memiliki arti terowongan, sesuai dengan namanya tunnel adalah sebuah jalur (terowongan) khusus yang dapat dilewati oleh data yang akan dikirim tanpa tergangu atau mengganggu data lain yang dilewatinya.

Tunneling adalah dasar dari VPN untuk membuat suatu jaringan private melalui jaringan internet. Tunneling juga merupakan enkapsulasi suatu protokol kedalam paket protokol. *Tunneling* menggunakan satu jaringan

untuk mengirim datanya melalui koneksi jaringan lain. *Tunneling* ini bekerja dengan mengenkapsulasi protokol jaringan dalam paket yang dibawa oleh jaringan public. (Rachmawan et al., 2018)

5. Point To Point Tunneling Protocol (PPTP)

Protokol Tunneling Point-to-Point adalah metode untuk meng-implementasikan VPN dengan banyak masalah keamanan yang diketahui dengan menggunakan saluran kontrol TCP dan saluran GRE (Generic Routing Encapsulation) untuk merangkum PPP (Protocol Point-to-Point).

Point to Point Tunneling Protocol (PPTP) adalah sebuah metode komunikasi data atau protokol yang memungkinkan terjadinya komunikasi anatara titik pada jaringan internet dengan membuat VPN. Pada metode PPTP, VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar komputer yang biasa disebut dengan client, baik komputer yang berada di kantor pusat maupun komputer yang berada di kantor cabang. Secara fisik server.

Sebuah VPN dapat berupa komputer (biasanya berupa sebuah personal computer / PC) yang sudah diinstall dan diset dengan perangkat lunak VPN atau dapat berupa sebuah router. (Supriyono et al., 2013)

6. Layer 2 Tunneling Protocol (L2TP)

L2TP atau Layer 2 Tunneling Protocol merupakan terowongan atau saluran yang aman (Tunnel Secure) yang gunanya untuk mengatur alur IP yang menggunakan PPP (Point-to-Point Protocol) untuk di-transmisikan melalui jaringan TCP/IP.

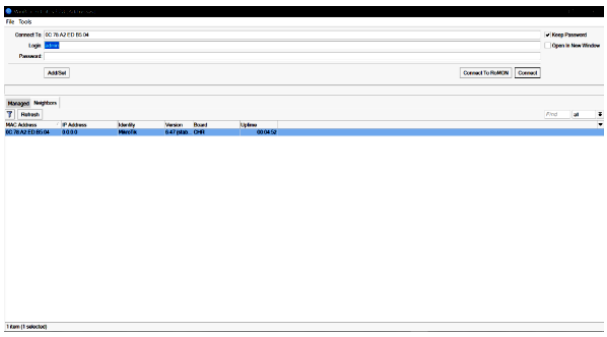
Layer 2 Tunneling Protocol adalah protocol tunneling yang digunakan untuk mendukung Virtual Private Network. L2TP juga merupakan tunnel standar dari satu router ke *router* lain atau dari *client* ke *host gateway* melewati *Network Access Server* (NAS) ISP yang dianalisa terlebih dahulu oleh server NAS ISP dan jika proses autentikasi berhasil maka ISP akan membuat saluran dari client ke host gateway secara Point-to-Point. L2TP merupakan basis dan kombinasi dari protokol L2F dari Cisco system dan PPTP dari Microsoft (Stiawan, 2005) dalam (Rachmawan et al., 2018).

III. METODE PENELITIAN

Metode yang digunakan mencegah Packet Sniffing pada suatu jaringan computer berbasis Mikrotik adalah dengan menerapkan keamanan VPN dengan metode L2TP/IPSec.

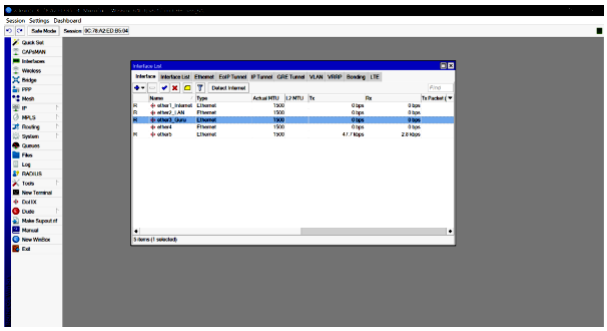
Konfigurasi yang diterapkan adalah sebagai berikut :

1. Login ke *router* mikrotik menggunakan Winbox.



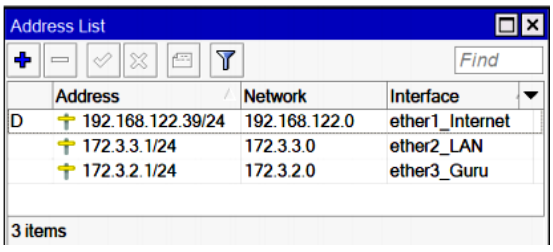
Gambar 1. Login Winbox

2. Ubah nama *interface* sesuai dengan kebutuhan.



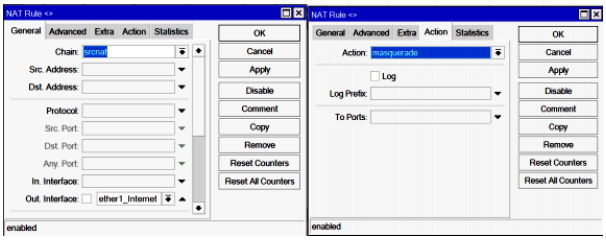
Gambar 2. Mengubah nama Interface

3. Beri IP Address untuk masing-masing Interface, dengan cara klik "IP > Addresses > klik tombol "+">lalu isikan IP Address sesuai dengan Interface.



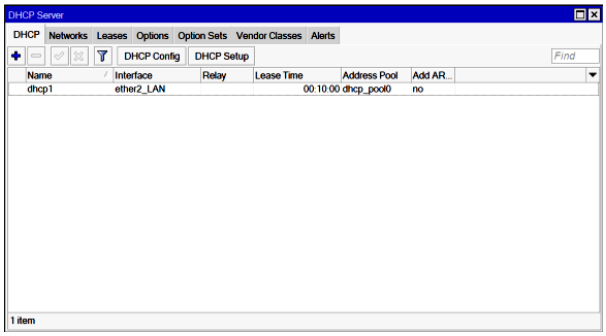
Gambar 3. Pemberian IP Address pada Interface

4. Aktifkan Firewall NAT pada Interface Internet dengan action Masquerade, dengan cara klik IP>Firewall>Tab NAT>klik tombol "+".kjhgkjdfh



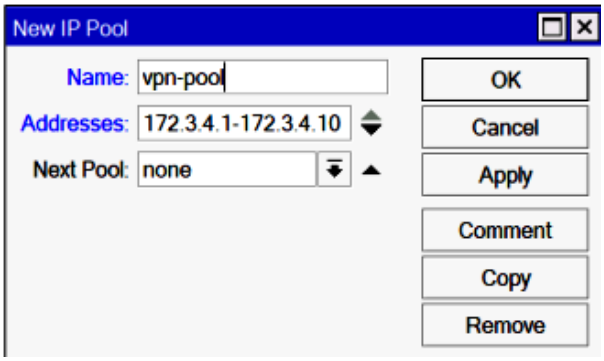
Gambar 4. Aktivasi Firewall pada Interface

5. Aktifkan DHCP server untuk Interface LAN, dengan cara klik IP>DHCP server > klik DHCP setup.



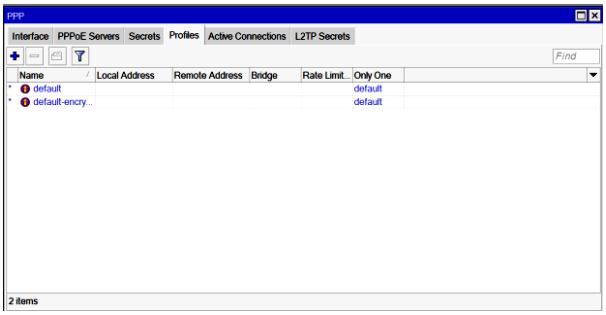
Gambar 5. Aktivasi DHCP Server

6. Setelah itu buat pool IP yang akan digunakan oleh VPN, dengan cara IP>Pool>klik tombol "+">sesuaikan addresses dengan kebutuhan.



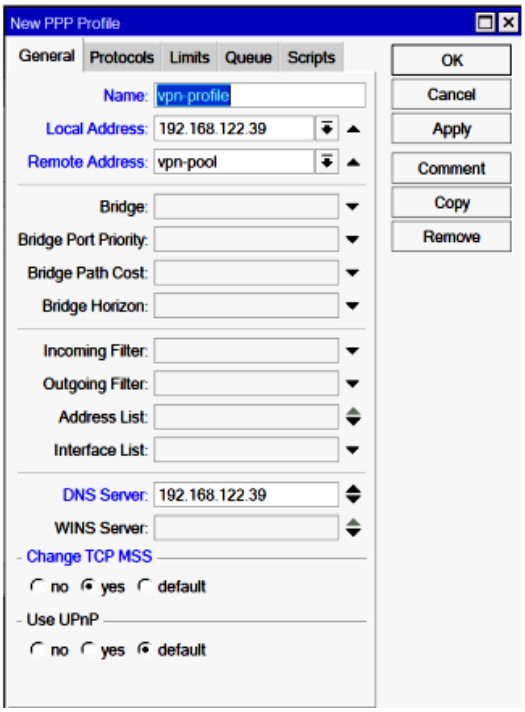
Gambar 6. Pembuatan IP Pool

7. Buat PPP profile yang akan digunakan oleh VPN, dengan cara klik menu PPP>tab Profiles > klik tombol "+".

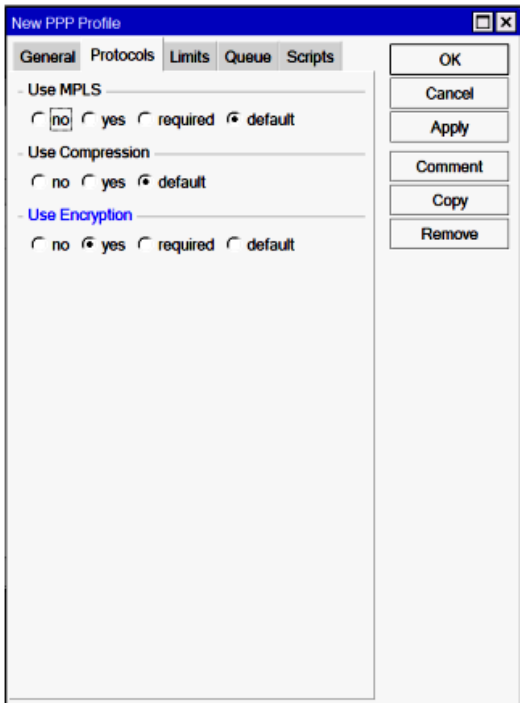


Gambar 7. Membuat PPP Profile

8. Selanjutnya pada kolom Name bisa bebas, pada kolom Local Address isikan IP Router, untuk Remote Address pilih vpn-pool yang sudah dibuat sebelumnya, DNS Server isi dengan IP router, klik yes pada Change TCP MSS, dan pada tab Protocols klik yes untuk Use Encryption lalu Apply dan OK.

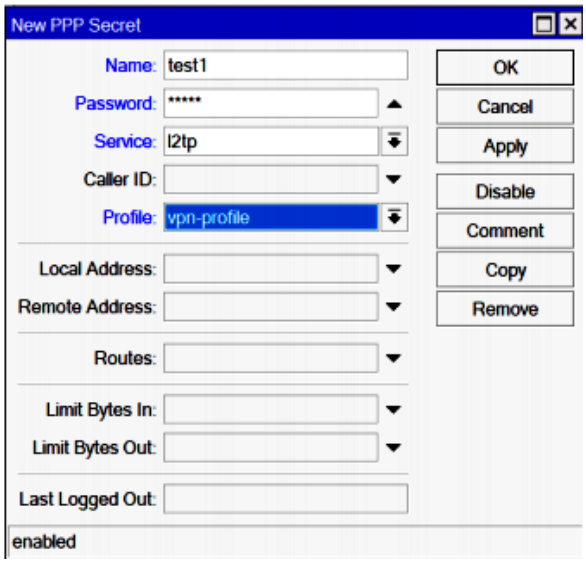


Gambar 8. Pemberian nama baru PPP Profile



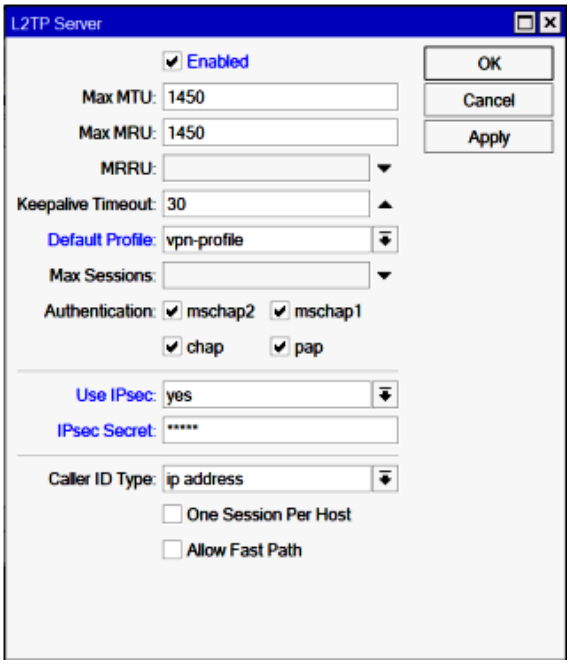
Gambar 9. Pemberian nama baru PPP Profile lanjutan

9. Sekarang kita bisa membuat VPN User, dengan cara PPP>tab Secrets> klik tombol "+". Pada kolom Name dan Password ini akan menjadi Username dan Password untuk VPN, pada parameter Service pilih l2tp, dan pada Profile pilih vpn-profile yang sudah di buat.



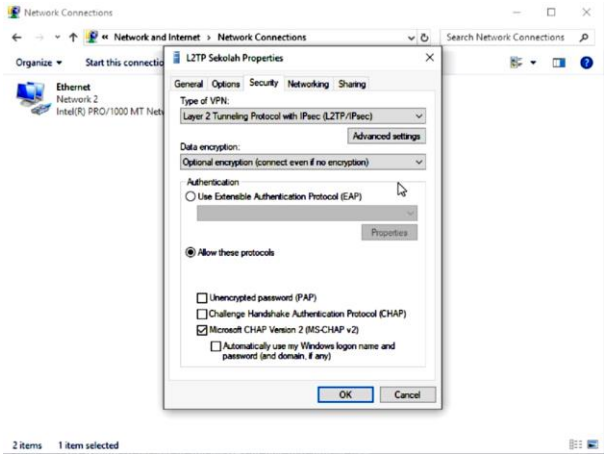
Gambar 10. Pemberian nama PPP Profile

10. Setelah itu saatnya mengaktifkan L2TP Server, dengan cara PPP>tab Interface > L2TP Server. Pastikan klik Enabled untuk mengaktifkan L2TP server, pada Default Profile pilih vpn-profile, kolom Use IPsec pilih yes, dan IPsec Secret sebagai kunci. Apply dan OK.



Gambar 11. Aktivasi LP2TP Server

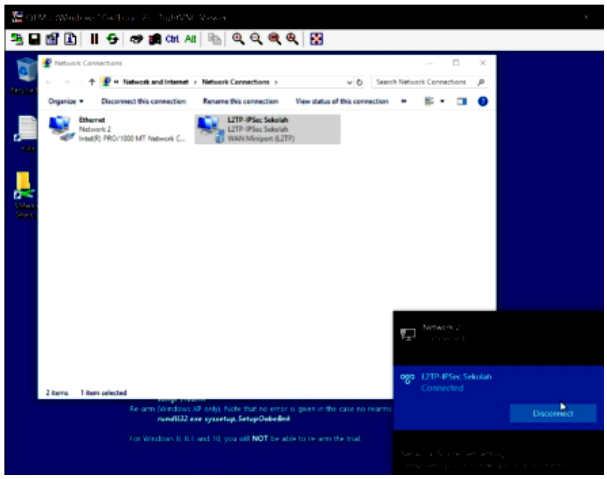
11. Sekarang PC sudah dapat terkoneksi ke VPN yang sudah di buat, dengan cara membuka Control Panel> Network and Interne t> Network and Sharing Center> lalu pilih Set up a new connection or network> Connect to a new workplace> Use my internet connection (VPN)> pada Internet Address isikan IP router mikrotik> lalu klik create> setelah itu ke change adapter setting> pilih properties pada network yang barusan di buat. Pada tab security klik advanced setting aktifkan use pre shared key for authentication dan masukan key nya.



Gambar 12. Setup koneksi baru

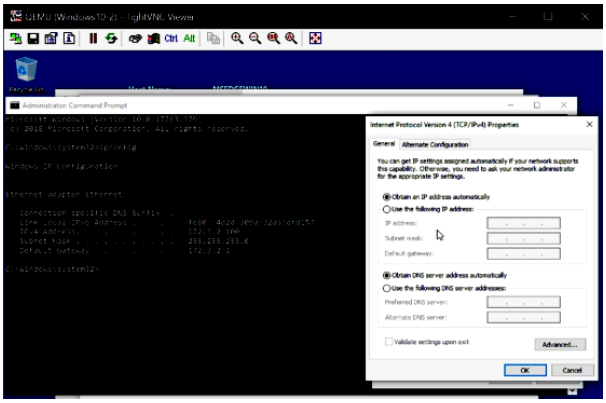
IV. HASIL PENELITIAN

Setelah dilakukan konfigurasi pada Router Mikrotik dengan metode VPN LP2TP/IPSec, dilakukan pengujian jaringan computer dengan hasil :



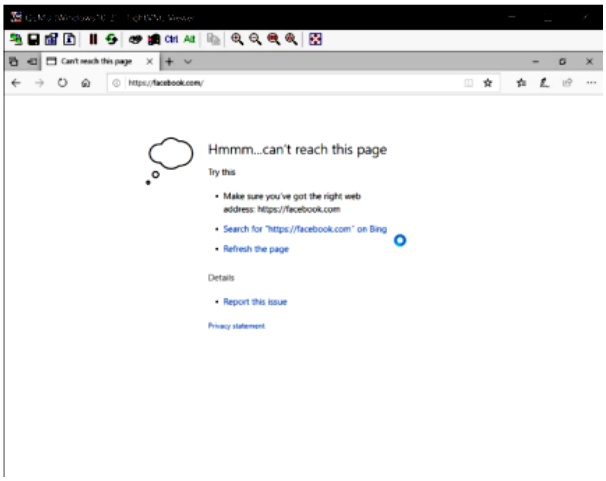
Gambar 13. Pengujian Jaringan Komputer yang sudah dikonfigurasi VPN LP2TP/IPSec

Pengujian pada DHCP Server, sehingga pada komputer client akan diberikan IP Address secara otomatis.



Gambar 14. Pengujian DHCP Server

Pengujian terhadap Firewall Filtering yang akan menolak akses kepada website-website yang tidak diinginkan atau tidak diijinkan untuk diakses oleh user.



Gambar 15. Pemblokiran Website dengan Firewall Filtering

V. KESIMPULAN

Setelah diterapkan konfigurasi VPN Tunnel dengan metode VPN LP2TP/IPSec untuk mencegah Packet Sniffing pada suatu jaringan computer berbasis Mikrotik, dapat ditarik kesimpulan sebagai berikut :

1. Dengan menambahkan konfigurasi VPN L2TP/IPSec pada mikrotik yang ada pada suatu jaringan komputer, keamanan jaringan akan menjadi lebih aman pada saat melakukan remote.
2. Dengan menerapkan DHCP Server untuk user pada suatu jaringan komputer, pemberian IP Address bisa dilakukan secara otomatis dan mengurangi resiko IP Collision.
3. Dengan diberlakukannya pemblokiran situs web, user tidak lagi bisa mengakses situs yang tidak ada kaitannya atau tidak diijinkan

DAFTAR PUSTAKA

Asteroid, K. M., & Hendrian, Y. (2016). ANALISIS WIRELESS LOCAL AREA NETWORK (WLAN) DAN PERANCANGAN MAC ADDRESS FILTERING MENGGUNAKAN MIKROTIK (STUDI KASUS PADA PT.GRAHA PRIMA SWARA JAKARTA). Jurnal Teknik Komputer, 2(2), 77–82.

Astuti, I. K. (2020). Jaringan Komputer. https://doi.org/10.31219/osf.io/p6ytb

Mahardiyanto, M. P., Suharto, N., & Darmono, H. (2016). Analisa Performansi Keamanan Jaringan Vpn Pptp Dan L2Tp/Ipsec Untuk Ftp Server Di Politeknik Negeri Malang. Jurnal Jartel: Jurnal Jaringan Telekomunikasi, 3(2), 32. http://jtdjurnal.polinema.ac.id/index.php/jtd/article/view/163

Maryanto, M., Maisyaroh, M., & Santoso, B. (2018). Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data. PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic, 6(2), 179–188. https://doi.org/10.33558/piksel.v6i2.1508

Pamungkas, D. P., Setiawan, A. B., & Ramadhani, R. A. (2020). Jaringan Komputer Dasar. In CV. Kasih Inovasi Teknologi.

Rachmawan, A., Prihanto, A., & Kom, M. (2018). Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN 53 Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet Di atas VPN. In Jurnal Manajemen Informatika (Vol. 8, Issue 2). https://jurnalmahasiswa.unesa.ac.id/index.php/jurnal-manajemeninformatika/article/view/24300

Rahadjeng, I. R., & Puspitasari, R. (2018). ANALISIS JARINGAN LOCAL AREA

NETWORK (LAN) PADA PT. MUSTIKA RATU Tbk JAKARTA TIMUR.

Rahman, T. (2017). Management Routing dengan Multiple Gateway dan GRE Tunnel. Jurnal Khatulistiwa Informatika, 5(2). https://doi.org/10.31294/JKI.V5I2.2890

Rohim, D. A., Karsono, K., & Mardiani, Y. (2016). Perancangan Sistem Informasi Penyewaan Mobil Pada CV. Surya Batara Tasikmalaya. Simnasiptek 2016, 1(1), 109–116.

Roma Doni, F. (2014). OPTIMALISASI JARINGAN WIRELESS DENGAN ROUTER MIKROTIK STUDI KASUS KAMPUS BSI TANGERANG. In EVOLUSI : Jurnal Sains dan Manajemen: Vol. II (Issue 1). http://www.bsi.ac.id

Siregar, T. I. (2019). Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan Packet Sniffing. Kumpulan Karya Ilmiah Mahasiswa Fakultas Sains Dan Tekhnologi, 1(1), 393–393. http://jurnal.pancabudi.ac.id/index.php/fastek/article/view/2201

Sujadi, H., & Burhanuddin, A. (2017). Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode Ipsec Vpn (Studi Kasus: Pt.Agrabudi Komunika). Infotech Journal, 3(2), 236702.

Sujadi, Harun, & Mutaqin, A. (2017). RANCANG BANGUN JARINGAN KOMPUTER TEKNOLOGI METROPOLITAN AREA NETWORK (MAN) DENGAN MENGGUNAKAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC) (Studi Kasus : Universitas Majalengka). J-ENSITEC. https://doi.org/10.31949/j-ensitec.v4i01.682

Supriyono, H., Widhaya, J. A., & Supardi, A. (2013). Penerapan Jaringan VPN Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami. Jarkom, 16(2), 88–101.

Varianto, E., & Badrul, M. (2015). Implementasi Virtual Private Network dan Proxy Server Menggunakan Clear OS Pada PT.Valdo International. Jurnal Teknik Komputer Amik Bsi, 1(1), 55–66.