Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol

Ria Andriani*, Ahmad Sa'di[2], Andriyan Dwi Putra[3]

[1,2]Fakultas Ilmu Komputer,Teknik Informatika, Universitas Amikom, Yogyakarta, Indonesia
[3]Fakultas Ilmu Komputer, Sistem Informasi, Universitas Amikom, Yogyakarta, Indonesia
Email: [1*]ria@amikom.ac.id, [2]ahmadsa@amikom.ac.id, [3]Andriyan.Putra@amikom.ac.id
Email Penulis Korespondensi: ria@amikom.ac.id
Submitted: **24/05/2022**; Accepted: **22/06/2022**; Published**: 30/06/2022**

Abstrak−Kantor XYZ adalah sebuah Instansi Pemerintah mencakup berbagai bidang, mulai dari pemerintahan, ekonomi, pembangunan, kesejahteraan rakyat, pembinaan kehidupan masyarakat serta urusan pelayanan umum. Namun kegiatan bekerja di instansi terganggu karena adanya pandemi COVID-19 yang menyebabkan pemerintah memberlakukan kebijakan Pembatasan Sosial Berskala Besar (PSBB) untuk menekan penyebaran virus ini sehingga mengakibatkan pekerja instansi harus bekerja dari rumah. Oleh karena itu dibutuhkan suatu sarana yang tepat untuk dapat mendukung kegiatan tersebut. Salah satunya adalah membuat rancangan teknologi dengan menerapkan VPN pada router mikrotik dengan metode PPTP *(Point to Point Tunnelling Protocol)* sehingga dapat mempermudah karyawan dalam berkomunikasi tanpa memikirkan lokasi, Selain itu user masih bisa melakukan remote access jaringan lokal meskipun berada di luar jaringan kantor selain itu keamanannya lebih terjamin.
Berdasarkan hasil pengujian terhadap keamanan jaringan di Kantor XYZ sebelum menggunakan VPN Server membuktikan bahwa penyadapan penyerang masih bisa memperoleh data berupa informasi login website, login mikrotik, maupun melihat isi data saat melakukan pertukaran data. Sedangkan Ketika user mengkoneksikan VPN Server penyadap tidak dapat melihat isi data di dalamnya, kemudian dengan adanya penerapan VPN dengan metode PPTP karyawan yang sedang bekerja dari rumah dapat saling terkoneksi dan berkomunikasi dengan baik, dengan itu pekerjaan dan pertukaraan informasi akan menjadi semakin fleksibel dan semakin cepat.

Kata Kunci: Mikrotik; Point to Point Tunneling Protocol; Virtual Private Network

Abstract−The XYZ office is a government agency covering various fields, ranging from government, economy, development, people's welfare, community life development and public service affairs. However, work activities in agencies were disrupted due to the COVID-19 pandemic which caused the government to impose a Large-Scale Social Restriction (PSBB) policy to suppress the spread of this virus, resulting in agency workers having to work from home. Therefore we need an appropriate means to be able to support these activities. One of them is making a technology design by implementing a VPN on a proxy router with the PPTP (Point to Point Tunnelling Protocol) method so that it can make it easier for employees to communicate without thinking about location. In addition, users can still remotely access the local network even though they are outside the office network. more secure. Based on the results of testing the network security at the XYZ Office before using the VPN Server, it proved that the wiretapping attackers could still obtain data in the form of website login information, proxy logins, or view data contents when exchanging data. Meanwhile, when the user connects to the VPN Server, the eavesdropper cannot see the contents of the data in it, then with the implementation of a VPN with the PPTP method, employees who are working from home can connect and communicate well with each other, with that work and information exchange will become more flexible and faster.

Keywords: Mikrotik; Point to Point Tunneling Protocol; Virtual Private Network

1. PENDAHULUAN

Kantor XYZ merupakan salah satu Instansi Pemerintah yang mencakup berbagai bidang, mulai dari bidang pemerintahan, ekonomi, pembangunan, kesejahteraan rakyat, pembinaan kehidupan masyarakat serta urusan pelayanan umum. Namun kegiatan bekerja di instansi terganggu karena adanya pandemi COVID-19 yang menyebabkan pemerintah memberlakukan kebijakan Pembatasan Sosial Berskala Besar (PSBB) untuk menekan penyebaran virus ini [1] sehingga mengakibatkan pekerja instansi harus bekerja dari rumah atau biasa disebut *Work From Home* (WFH). Kondisi ini menyulitkan karyawan dalam proses pertukaran data maupun konsolidasi data.

Proses penyimpanan data menjadi tidak terorganisir dan terpusat, apalagi dimasa pandemi karyawan tidak dapat mengakses sumber daya jaringan yang sama dengan saat karyawan berada dilokasi. Kemudian dalam sebuah jaringan komputer keamanan didalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga atau pihak yang tidak berkepentingan, terutama jika data tersebut bersifat rahasia atau penting. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan, salah satunya adalah menggunakan VPN atau *Virtual Private Network* dengan metode PPTP (Point to Point Tunneling Protocol). Dalam implementasinya, VPN terbagi menjadi remote access VPN dan site-to-site VPN. Remote access VPN digunakan sebuah perusahaan untuk para pekerjanya yang membutuhkan koneksi ke jaringan mereka dari berbagai lokasi atau memungkinkan pekerja untuk mengakses data-data dan segala sumber daya dimanapun mereka berada. Penelitian sejenis yang membahas tentang Implementasi VPN sudah banyak dilakukan, Penelitian pertama oleh Elly Mufida dkk (2017), Penelitian ini bertujuan untuk mempermudah dalam proses integrasi data terutama berkaitan dengan keuangan siswa pada masing-masing sekolah. Di dalam penelitiannya diperoleh hasil jaringan kantor Yayasan dengan jaringan sekolah dapat terhubung melalui jalur tunneling , Lalu proses pengambilan data sudah tidak lagi ditarik secara manual atau menggunakan email tetapi sudah dengan jaringan VPN , Kemudian sistem jaringan

Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

VPN jauh lebih aman dan dana yang dibutuhkan dalam pembangunan sistem jaringan VPN dengan router mikrotik lebih terjangkau.[2]

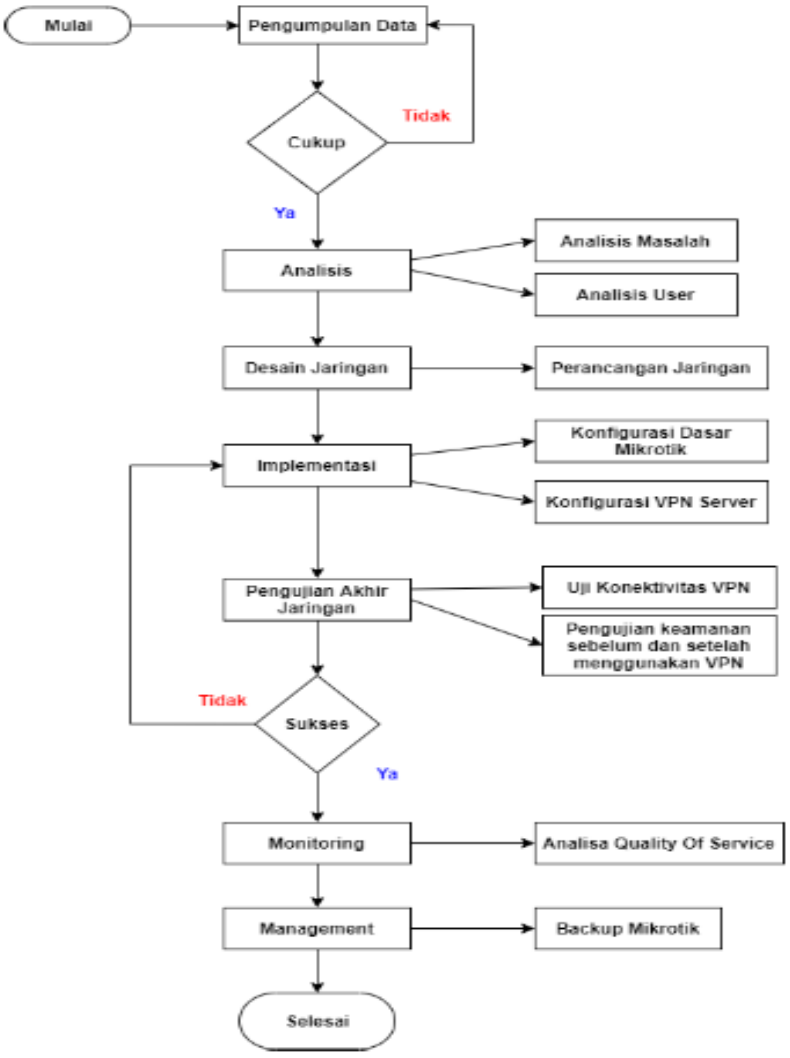
Penelitian selanjutnya dilakukan oleh Haekal Alief Syawaludin, dkk (2020), Penelitian ini bertujuan untuk menghubungkan server pusat agar dapat diakses oleh Gedung sekolah SMP dan SMK dengan tingkat keamanan sama seperti konsep jaringan LAN *(Local Area Network*) di mana data hanya dapat diakses bila seorang terhubung dengan jaringan pusat, Gedung SMP atau Gedung SMK saja di luar dari ini maka tidak akan dapat mengakses server tersebut. Kemudian diperoleh hasil dengan adanya tunneling PPTP VPN maka pengiriman informasi dan data antar instansi pusat dengan cabang tidak perlu menggunakan aplikasi pihak ketiga karena sudah menggunakan jalur khusus untuk mengirim informasi dengan cepat,aman dan mudah. dan dapat mempermudah pengguna pada instansi cabang untuk mengakses server pada instansi pusat meskipun pada lokasi yang berjauhan.[3]

Penelitian selanjutnya dilakukan oleh S. Dewi (2020), Penelitian ini bertujuan agar pertukaran data dari kantor kabupaten ke kantor desa dapat dilakukan secara aman dan terkendali, kemudian disebutkan bahwa metode tunneling protocol PPTP *(Point to Point Tunneling Protocol)* yang diterapkan pada Kantor Desa Kertaharja berdampak sangat positif karena dengan adanya penerapan metode tunneling tersebut jaringan komputer antara kantor dapat saling terhubung dan berkomunikasi, dengan itu pekerjaan dan pertukaran informasi akan menjadi semakin fleksibel dan semakin cepat, dan juga administrator jaringan tidak perlu repot-repot melakukan kunjungan untuk memonitoring jaringan yang sedang berjalan pada masing-masing kantor. [4]

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Untuk mempermudah penulis dalam merancang, menerapkan dan menentukan hasil dari penelitian maka, sistematika penelitian juga harus terstruktur dan memiliki alur, Adapun alur penelitian yang akan dilakukan oleh penulis dapat dilihat pada Gambar 1. berikut.



Gambar 1. Alur Penelitian

Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

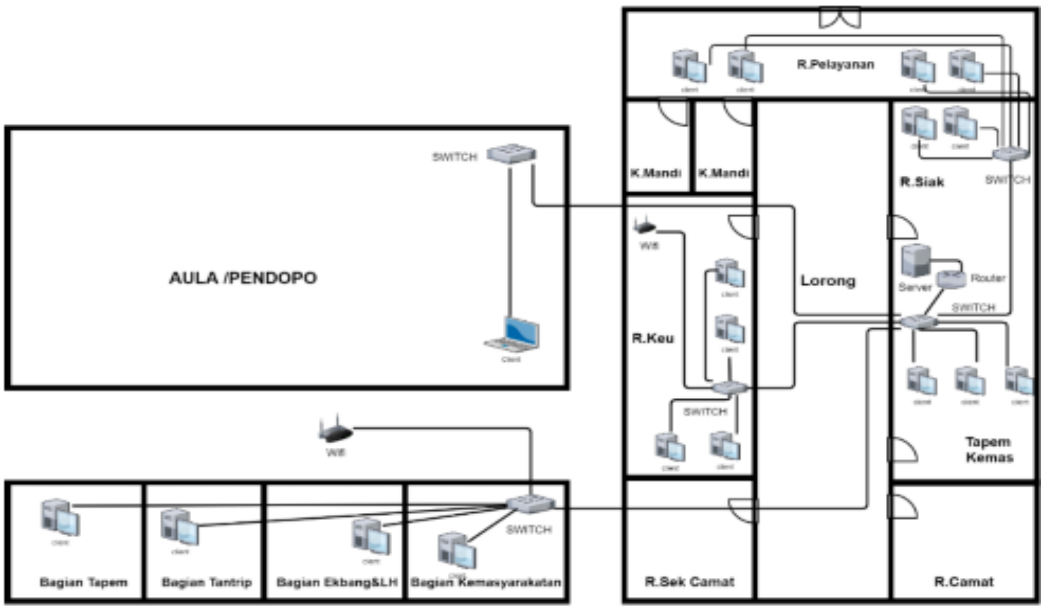
Pada gambar alur penelitian, metode penelitian ini menggunakan metode NDLC *(Network Development Life Cycle)* yang membutuhkan beberapa tahapan berupa analisa masalah, pengumpulan data, desain jaringan, implementasi, pengujian akhir jaringan, monitoring, dan Management.

a. Pengumpulan Data

Pada tahap ini penulis melakukan pengumpulan data, baik data dari lapangan dan data sampling beberapa titik jaringan free wifi publik yang di bantu oleh tim NOC. Dari data – data tersebut nantinya akan di olah di tahap pengolahan data. Adapun data yang dimaksud yaitu berupa perangkat keras yang digunakan, denah jaringan yang ada, serta topologi yang berjalan

b. Analisis

Pada tahap ini penulis melakukan analisa terhadap topologi yang tersedia pada kantor XYZ, dimana denah jaringannya dapat dilihat pada Gambar 1 berikut.

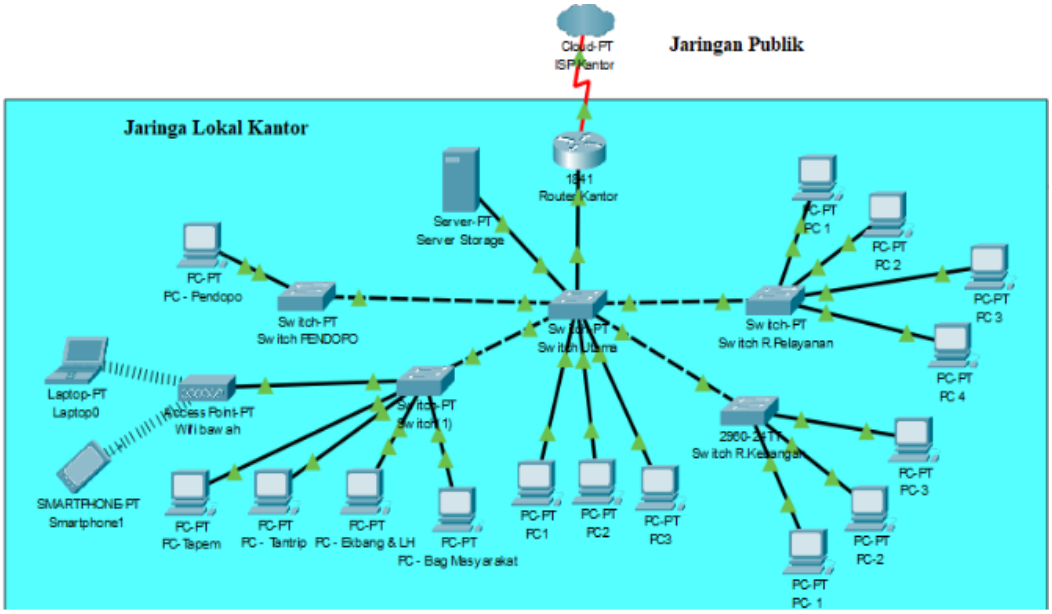


Gambar 2. Denah Jaringan Kantor XYZ

Pada gambaran denah jaringan di Kantor XYZ dapat dilihat bahwa dari ISP yang digunakan diteruskan ke router dan didistribusikan jaringan ke setiap ruangan menggunakan switch. Dari switch tersebut kemudian didistribusikan ke beberapa perangkat dan access point.

c. Perancangan Jaringan

Rancangan jaringan sebelum menggunakan VPN pada kantor XYZ dapat dilihat pada Gambar 2 berikut ini.

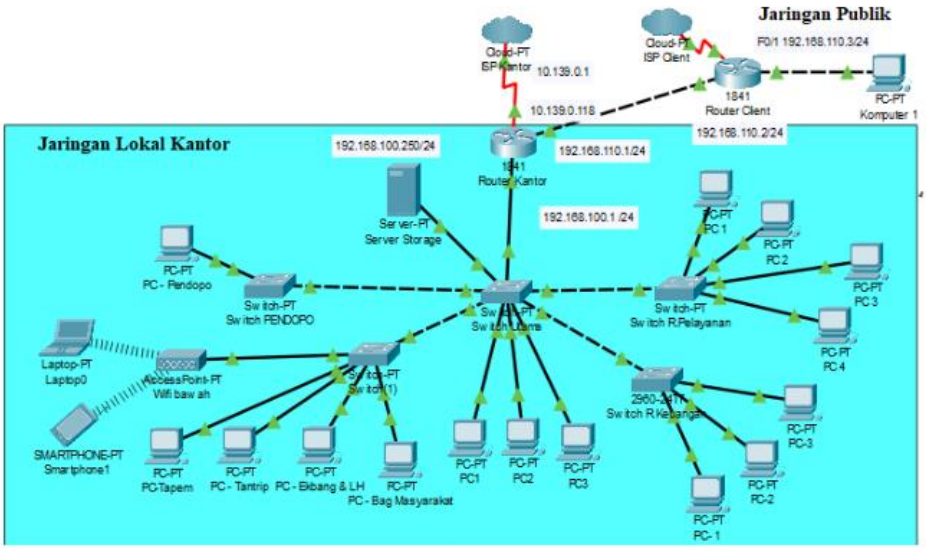


Gambar 3. Topologi Jaringan Kantor XYZ

Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

Jika diperhatikan desain jaringan pada gambar 2, terlihat bahwa alur jaringan bermula dari *Router Internet Service Provider* (ISP) menuju Switch pusat yang terhubung ke Server Storage dan Switch-Switch yang lain, kemudian client terhubung ke end device seperti PC , Laptop, Handphone melalui Access Point.

Setelah mendesain topologi jaringan di Kantor XYZ , penulis melakukan perubahan jaringan yang sudah ada dengan menambahkan Mikrotik tipe RB941 yang berfungsi sebagai VPN Server. Seperti yang ditunjukkan pada Gambar 3 berikut.



Gambar 4. Rancangan Baru Topologi Kantor XYZ

Pada desain jaringan baru, penulis merancang sebuah Router Mikrotik untuk diletakkan diantara Switch Pusat dan Router ZTE F609 yang difungsikan sebagai gateway,firewall dan VPN Server , kemudian untuk mengakses jaringan VPN melalui jaringan public atau internet dari luar jaringan kantor ditunjukkan pada gambar 3 diatas.

Adapun data perangkat beserta IP Address dapat dilihat pada table 1 berikut.

Tabel 1. Daftar Perangkat Dan Ip Address

No	Hardware	Ip Address	Subnet Mask
1	Router ISP ZTE F609	10.139.0.1	255.255.255.0
2	Mikrotik RB941-2nd	LAN 1 : 10.139.0.118/24	255.255.255.0
		LAN 2 : 192.168.100.1/24	255.255.255.0
3	VPN Server	192.168.110.1/24	255.255.255.0
4	Server Storage	192.168.100.250/24	255.255.255.0
5	Wifi Bawah	192.168.100.50/24	255.255.255.0

Keterangan pembagian alamat IP pada tabel 1 di atas adalah sebagai berikut:

1. IP 10.139.0.1 untuk Router bawaan ISP ZTE F609 yang terhubung internet pada posisi sebelum RB 941-2nd
2. IP 10.139.0.118 merupakan IP Address DHCP Server yang terhubung pada Mikrotik RB posisi setelah ISP Kantor berbasis kabel (LAN), berfungsi sebagai gateway,firewall,dan VPN Server.
3. IP 192.168.100.1 merupakan IP lokal kantor XYZ yang kemudian akan di DHCP Server untuk perangkat dibawahnya
4. IP 192.168.100.250 untuk Server Storage terhubung pada posisi setelah Switch Utama dan RB 941, yang berfungsi sebagai tempat penyimpanan data dari semua client.
5. IP 192.168.110.1 merupakan IP VPN Server yang nantinya akan dijadikan DHCP Server untuk client yang terhubung melalui VPN Client
6. IP 192.168.100.50 untuk Router Wireless pada Ruang Pendopo terhubung pada posisi setelah Switch Utama dan RB 941

d. Skenario Pengujian

Pada tahap pengujian, Mikrotik RB941 berfungsi sebagai alat untuk membuat VPN Server. Berikut adalah skenario pengujian yang akan dilakukan.

a. Pengujian keberhasilan koneksi VPN Server dan akses file server melalui jaringan publik.
b. Pengujian keamanan *Virtual Private Network* (VPN) dengan metode *Point to Point Tunneling protocol* (PPTP) meliputi serangan sniffing pada saat user melakukan login website , login perangkat mikrotik, dan pengiriman file ke server. Kemudian akan dibandingkan keamanan sebelum dan setelah menggunakan VPN Server.
e. Monitoring

Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

Tahap pengamatan merupakan tahapan yang penting agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan rencana awal pada tahap analisis, maka perlu dilakukan kegiatan monitoring atau pengamatan dengan memanfaatkan fitur traffic pada mikrotik itu sendiri.

f. Management
Tahapan dari metode pengembangan NDLC berikutnya adalah manajemen, Manajemen perlu dibuat untuk mengatur dan membuat sistem yang telah dibuat dapat terjaga dengan baik sehingga diperlukan backup konfigurasi dan log monitoring
1. Backup konfigurasi dilakukan untuk mencegah bila terjadi kerusakan pada perangkat keras atau hal yang tidak diinginkan.
2. Log monitoring dilakukan untuk mengetahui proses apa saja yang telah dilakukan router mikrotik tersebut dan dengan menganalisa log monitoring mempermudah kita dalam menemukan masalah dan menerapkan solusinya.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian Konektifitas Pada VPN Server dan File Server

Adapun hasil pengujian pada sistem yang telah berhasil dilakukan dapat dilihat pada table 2 berikut ini.

Tabel 2 Hasil Pengujian Konektivitas VPN Server

No	Skenario Pengujian Sistem	Uji Coba	Hasil yang Diharapkan	Hasil pengujian	Kesimpulan
1	Koneksi VPN	Koneksi Melalui VPN Client	Terhubung	Terhubung	Berhasil
2	Koneksi File Server	Koneksi Melalui File Server	Terhubung	Terhubung	Berhasil

Pada Tabel 2 di atas dapat dijelaskan bahwa hasil dari pengujian konektivitas pada VPN Server tersebut telah berhasil mulai dari pengujian system sampai hasil yang di harapkan telah terhubung, Maka kesimpulan dari pengujian konektivitas VPN Server tersebut telah berhasil dilakukan. Selain dapat menghubungkan jaringan lokal di Kantor XYZ melalui jaringan public atau internet , VPN Server juga memberikan keamanan yang lebih baik sehingga tidak ada data yang dapat dicuri dengan mudah.

3.2 Hasil Perbandingan Keamanan Sebelum dan Sesudah VPN

Dalam hasil pengujian pada serangan yang telah penulis lakukan, berikut ini adalah hasil pengujian keamanan jaringan sebelum dan setelah menggunakan VPN Server yang telah berhasil dilakukan :

Tabel 3. Hasil Perbandingan Keamanan Sebelum dan Setelah

No	Skenario Pengujian Sistem	Sebelum Menggunakan VPN	Setelah Menggunakan VPN
1	User Melakukan Login Website	Username dan Password yang dimasukkan user dapat dilihat penyerang	Tidak ada paket yang dapat dibaca penyerang
2	Admin Jaringan Melakukan Login Mikrotik WebFig	Username yang dimasukkan admin jaringan dapat dilihat penyerang	Tidak ada paket yang dapaT dibaca penyerang
3	User Mengirimkan File Ke Server Storage	Koneksi Melalui File Server	Tidak ada paket yang dapat dibaca penyerang

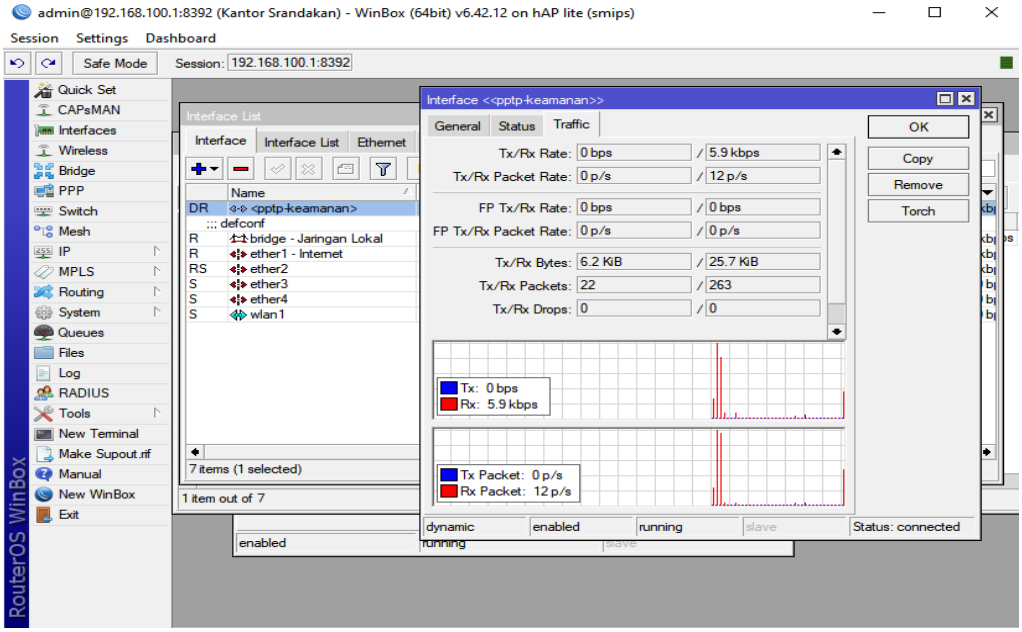
Dalam Tabel 3 dijelaskan bahwa hasil pengujian pada 3 skenario penyerangan menggunakan Wireshark yaitu disaat user melakukan Login Website didapat hasil sebelum menggunakan VPN Server, Username dan Password yang dimasukkan user dapat dilihat penyerang. Setelah menggunakan VPN Server tidak ada paket yang dapat dibaca penyerang. Kemudian untuk hasil pengujian pada saat admin jaringan melakukan login Mikrotik menggunakan WebFig didapat hasil sebelum menggunakan VPN Server, Username yang dimasukkan admin jaringan dapat dilihat penyerang. Setelah menggunakan VPN Server tidak ada paket yang dibaca penyerang. Selanjutnya untuk hasil pengujian pada saat user mengirimkan file ke Storage Server didapat hasil sebelum menggunakan VPN Server, Nama dan isi file dapat dilihat penyerang. Setelah menggunakan VPN Server tidak ada paket yang dapat dibaca oleh penyerang. Hal ini membuktikan dengan menggunakan VPN Server lebih aman dibanding tidak menggunakan sama sekali , dikarenakan koneksi VPN menggunakan protocol TCP port 1723, dan menggunakan IP Protocol 47/GRE

Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

untuk enkapsulasi datanya , Untuk proses autentikasi PPTP menggunakan mschap2. Setelah tunnel terbentuk , data yang ditransmisikan akan di enkripsi menggunakan Microsoft Point-to-Point Encryption (MPPE).

3.3 Monitoring

Tahap pengamatan merupakan tahapan yang penting agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan rencana awal pada tahap analisis, maka perlu dilakukan kegiatan monitoring atau pengamatan dengan memanfaatkan fitur traffic pada mikrotik itu sendiri.



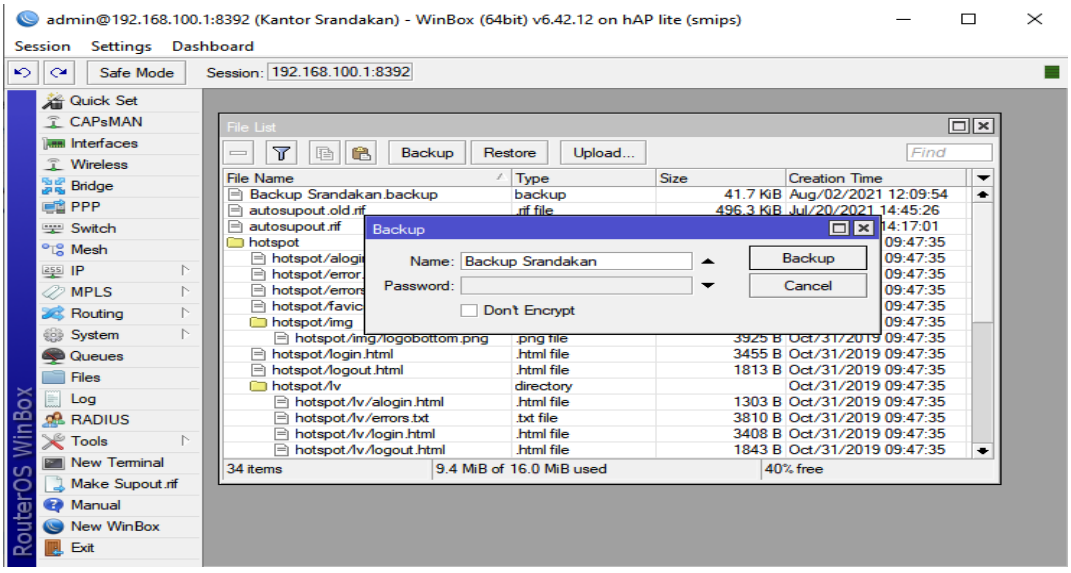
Gambar 4. Monitoring Kondisi Jaringan Knator XYZ

Pada Gambar 4 di atas dapat dijelaskan bahwa dengan menggunakan mikrotik kita dapat melihat traffic yang berjalan , serta admin jaringan dapat melakukan monitoring.

3.4 Manajemen

Manajemen perlu dibuat untuk mengatur dan membuat sistem yang telah dibuat dapat terjaga dengan baik sehingga diperlukan backup konfigurasi dan log monitoring.

a. Backup konfigurasi dilakukan untuk mencegah apabila terjadi kerusakan pada perangkat keras atau hal yang tidak diinginkan terjadi

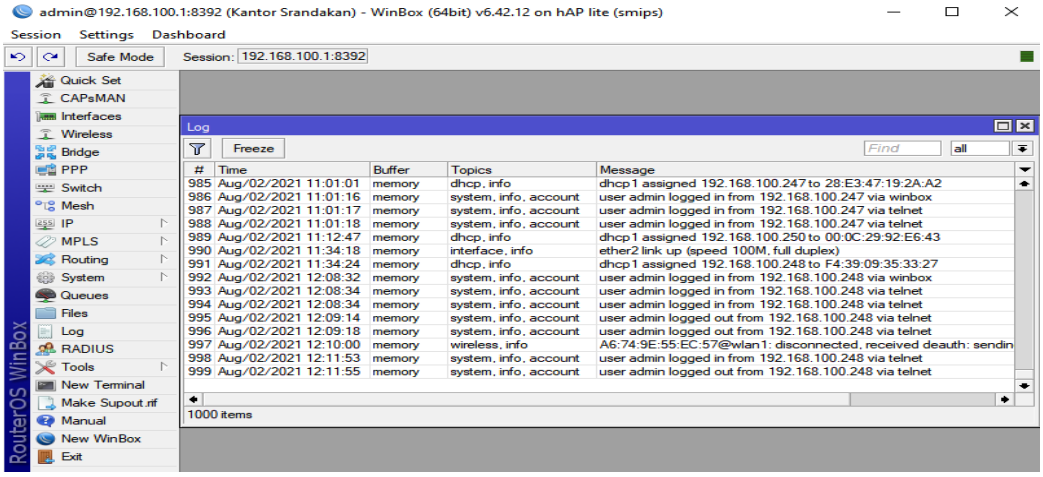


Gambar 5. Backup Konfigurasi Mikrotik

Dari Gambar 5 di atas dapat dijelaskan bahwa penting untuk melakukan backup konfigurasi agar ketika terjadi kerusakan pada hardware maupun konfigurasi yang salah dapat di backup, sehingga administrator jaringan dapat dengan cepat memperbaiki kerusakan yang terjadi.

Building of Informatics, Technology and Science (BITS)
Volume 4, No 1, Juni 2022 Page: 184−190
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i1.1611

b. Log monitoring dilakukan untuk mengetahui proses apa saja yang dilakukan oleh router mikrotik tersebut dan dengan menganalisa log monitoring dapat mempermudah kita dalam menemukan masalah dan menerapkan solusinya.



Gambar 6. Log system pada mikrotik

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan dari metode yang diterapkan oleh penulis dalam mengatasi permasalahan yang terjadi maka dapat ditarik kesimpulan bahwa, Selama User terkoneksi dengan internet dan memiliki hak akses maka client dapat meremote dan mengakses file server di kantor XYZ dari mana saja. Selain itu dengan adanya penerapan VPN dengan metode PPTP, memudahkan karyawan Kantor XYZ yang sedang bekerja dari rumah atau *work from home* dapat saling berkomunikasi, sehingga pekerjaan dan pertukaran informasi akan menjadi semakin fleksibel dan semakin cepat. Serta pengujian keamanan terhadap jaringan di kantor XYZ sebelum menggunakan VPN Server membuktikan bahwa penyadap masih bisa memperoleh data berupa informasi login website, login mikrotik, maupun melihat isi data ketika melakukan pertukaran data. Sedangkan ketika user mengkoneksikan VPN Server penyadap tidak dapat melihat isi data yang terdapat di dalamnya.

REFERENCES

[1] R. Kemenkes, “Keputusan Menteri Kesehatan Republik Indonesia Nomor HK.01.07/MenKes/413/2020 Tentang Pedoman Pencegahan dan Pengendalian Corona Virus Disease 2019 (Covid-19),” MenKes/413/2020, vol. 2019, p. 207, 2020.
[2] E. Mufida, D. Irawan, and G. Chrisnawati, “Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta,” J. Matrik, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.
[3] L. Auditya, C. Kartiko, and C. Wiguna, “Jurnal Edik Informatika Jurnal Edik Informatika,” Penelit. Bid. Komput. Sains dan Pendidik. Inform., vol. 7, no. 1, pp. 9–18, 2020.
[4] S. Dewi, “Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis,” EVOLUSI J. Sains dan Manaj., vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.
[5] Y. Putra, Jordy Lesmana, Indriyani, Luthfi, Angraini, “Penerapan Sistem Keamanan Jaringan Menggunakan,” IJCIT (Indonesian J. Comput. Inf. Technol., vol. 3, no. 2, pp. 260–267, 2018.
[6] S. Watmah, “Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang,” Insa.– J. Inov. dan Sains Tek. Elektro ISSN 2722-574X, vol. 1, no. 1, pp. 6–12, 2020.
[7] T. Rahman, “Implementasi Virtual Private Network,” J. Ilmu Pengetah. dan Teknol. Komput., vol. 3, no. 1, pp. 1–12, 2017.
[8] R. Toyib, M. Muntahanah, and J. Prima, “Pemanfaatan Vpn Dengan Ip Cloud Mikrotik Menggunakan Jaringan 3G (Studi Kasus : Pt. Bprs Muamalat Harkat Bengkulu),” Sistemasi, vol. 8, no. 1, p. 90, 2019, doi: 10.32520/stmsi.v8i1.428.
[9] I. K. Susila and I. M. Sukafona, “Analisis Quality Of Service Jaringan Virtual Private Network (VPN) di STMIK STIKOM Indonesia,” 2019.
[10] A. W. Santosa, “Implementasi Freenas Sebagai Penyimpanan pada Proxmox Menggunakan Metode Failover: Server Freenas,” 2017.
[11] H. Supendar, “Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik,” Bina Insa. ICT J., vol. 3, no. 1, p. 234340, 2016.
[12] Afrianto and E. B. Setiawan, "Kajian Virtual Private Network (VPN) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom)," Jurnal Majalah Ilmiah Unikom, vol. Vol. 12, pp. 43-52, 2014.
[13] Anwar, R. S., & Agustina, N. (2020). Implementasi dan Analisa Kinerja Jaringan Wide Area Network dengan Open VPN-Access Server. 4(2), 143–152.
[14] Arnita, A., & Farid, M. (2020). Implementasi jaringan virtual private network dengan teknologi Multi Protocol Label Switching (MPLS). 5(2), 28–39
[15] Zarkasyi, M. H., Agus, I., Permana, G., Dillak, H. C., & Kom, S. (2018). Implementasi Virtual Private Network (Vpn) Server Dengan Menggunakan Mikrotik Os Di Pt . Charisma Persada, 4(3), 2463–2474.