p-ISSN: 2301-6949
e-ISSN : 2715-5064

Perancangan *Virtual Private Network* Dengan Protokol PPTP Menggunakan MikroTik Untuk Kebutuhan *Remote Access*

Vicky Phang[1], **Endah Setyaningsih**[2*)]
[12]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Tarumanagara, Jakarta
[12]Jln. Letjen S. Parman No. 1, Kota Jakarta Barat, 11440, Indonesia
email: [1]vicky.525180001@stu.untar.ac.id, [2]endahs@ft.untar.ac.id

Abstract* – *Internet has become an essential requirement for communication. By using the internet, it is possible for someone to get information anytime and anywhere. The internet is also used in local networks. The local network connects personal devices and workstations in an organization for the use of shared resources. The local network cannot be accessed from outside carelessly. A Virtual Private Network (VPN) allows devices outside the local network to connect using a public network anywhere on the condition that the device is connected to the internet. Therefore, in this journal a VPN network with a Point-to-Point Tunneling Protocol (PPTP) is designed using a MikroTik router. The PPTP protocol adds data security in these networks. A VPN network is designed to connect a total of two computers, one in the local network and one outside the local network. The VPN account that is created is for one device only. Computers on the local network use the Windows 10 operating system while computers outside the network use the Windows 7 operating system. Devices on the local network are connected using a straight type UTP cable with an RJ45 connector. The router used is the MikroTik hAP lite RB941-2nd router. The router is connected to a public network with an IP address of 103.83.174.25. The media used to configure the MikroTik router is WinBox version 3.27 (64-bit).

Keywords* – *VPN, PPTP, MikroTik, Remote Access.

Abstrak* – Internet telah menjadi kebutuhan yang penting untuk berkomunikasi. Dengan menggunakan internet dimungkinkan seseorang untuk mendapatkan informasi kapan saja dan di mana saja. Internet juga digunakan dalam jaringan lokal. Jaringan lokal menghubungkan perangkat-perangkat pribadi dan *workstation* dalam suatu organisasi untuk pemakaian sumber daya bersama. Jaringan lokal tidak dapat diakses dari luar secara sembarangan. *Virtual Private Network* (VPN) memungkinkan perangkat di luar jaringan lokal untuk terhubung dengan menggunakan jaringan publik di mana saja dengan syarat perangkat terhubung ke internet. Oleh karena itu, pada jurnal ini dirancang jaringan VPN dengan protokol *Point-to-Point Tunneling Protocol* (PPTP) menggunakan *router* MikroTik. Protokol PPTP menambah keamanan data dalam jaringan tersebut. Jaringan VPN yang dirancang menghubungkan total dua komputer, satu berada dalam jaringan lokal dan satu lagi di luar jaringan lokal. Akun VPN yang dibuat hanya diperuntukkan satu perangkat. Komputer pada jaringan lokal menggunakan sistem operasi Windows 10 sedangkan komputer di luar jaringan menggunakan sistem operasi Windows 7 Perangkat pada jaringan lokal terhubung menggunakan kabel UTP tipe *straight* dengan konektor RJ45. Router yang digunakan adalah *router* MikroTik hAP *lite* RB941-2nd. *Router* terhubung ke jaringan publik dengan alamat IP 103.83.174.25. Media yang digunakan untuk mengonfigurasi *router* MikroTik adalah WinBox versi 3.27 (64-bit).

***Kata Kunci* – VPN, PPTP, MikroTik, *Remote Access*.**

I. PENDAHULUAN

Jaringan lokal adalah salah satu jenis jaringan komputer yang menghubungkan perangkat komputer dan *workstation* dalam suatu organisasi, perusahaan atau kantor-kantor dengan tujuan pembagian sumber daya [1]. Perangkat dalam jaringan lokal kantor terhubung menggunakan kabel atau tanpa kabel. Menghubungkan perangkat yang jaraknya jauh ke jaringan lokal menggunakan infrastruktur pribadi menghabiskan biaya yang besar [2]. Selain biayanya yang besar, faktor keamanan juga menjadi pertimbangan penting, mengingat adanya data yang bersifat sensitif yang hanya boleh diketahui atau digunakan oleh orang yang berkepentingan dalam jaringan lokal tersebut [3]. Oleh karena itu, tidak sembarang orang dapat mengakses data dalam jaringan lokal.

Berdasarkan permasalahan di atas, maka dilakukan perancangan *Virtual Private Network* (VPN) dengan protokol *Point-to-Point Tunneling Protocol* (PPTP) menggunakan MikroTik. *Virtual Private Network* (VPN) merupakan sebuah sistem komunikasi pada jaringan komputer yang memungkinkan suatu perangkat terhubung ke jaringan lokal tanpa harus terhubung langsung dengan menggunakan infrastruktur jaringan publik sehingga jaringan lokal dapat diakses secara *remote*[4]. Dengan menggunakan VPN, dimungkinkan untuk membuat perangkat di luar jaringan lokal untuk terhubung dengan suatu jaringan lokal secara virtual seolah-olah perangkat di luar jaringan lokal terhubung secara fisik dengan jaringan lokal tersebut. Penggunaan protokol PPTP juga meningkatkan keamanan data sehingga data hanya dapat diakses oleh pengguna VPN.

Tujuan perancangan ini adalah untuk merancang *Virtual Private Network* (VPN) dengan menggunakan *router* MikroTik hAP *Lite* sebagai VPN Server dan menggunakan protokol keamanan *Point-to-Point Tunneling Protocol* (PPTP). VPN yang dirancang menghubungkan 2 perangkat komputer dengan sistem operasi Windows 7 dan Windows 10.

*) **penulis korespondensi**: Endah Setyaningsih
Email: endahs@ft.untar.ac.id

II. PENELITIAN YANG TERKAIT

Ikhwan dan Uray dalam penelitiannya mengimplementasikan *Virtual Private Network* (VPN) menggunakan protokol *Secure Socket Tunneling Protocol* (SSTP) dan perangkat MikroTik pada Fakultas MIPA Universitas Tanjungpura. Latar belakang masalahnya adalah semakin bertambahnya jumlah mahasiswa sehingga akses

internet menjadi lambat, terutama pada Fakultas MIPA. Akses internet pada Fakultas MIPA terbuka untuk umum sehingga rentan atau mudah diakses oleh pihak yang tidak berkepentingan. Dengan menggunakan VPN pada fakultas MIPA Universitas Tanjungpura, maka dapat mempercepat akses internet dan memaksimalkan penggunaan akses internet pada Fakultas MIPA, serta memaksimalkan keamanan akses internet pada Fakultas MIPA [5]. Sistem Operasi yang digunakan pada komputer *client* adalah Windows 7. Media WebFig/Browser digunakan untuk mengonfigurasi VPN.

Heri pada penelitiannya merancang jaringan VPN menggunakan MikroTik RB951 pada Satuan Brimob Polda Jawa Timur. Protokol VPN yang digunakan Heri adalah *Layer 2 Tunneling Protocol* (L2TP). Tujuan perancangan ini untuk membantu Satuan Brimob Polda Jawa Timur membuat jaringan pribadi yang memanfaatkan jaringan publik atau internet untuk menghubungkan antara *remote-site* secara aman [6]. Sistem Operasi yang digunakan pada komputer *client* adalah Windows 8. Media WinBox digunakan untuk mengonfigurasi VPN.

Adapun perbandingan hasil penelitian sebelumnya dengan perancangan ini yang dapat dilihat pada Tabel I. Terdapat 4 parameter yang digunakan sebagai acuan pembandingan, yaitu protokol VPN yang digunakan, *router* yang digunakan, OS komputer *client* dan media untuk mengonfigurasi VPN.

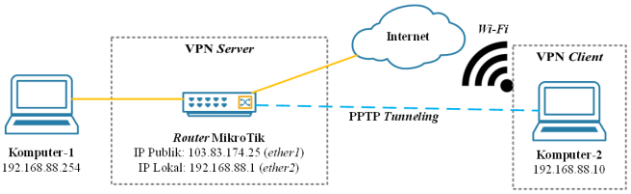
TABEL I
PERBANDINGAN PENELITIAN SEBELUMNYA DENGAN ALAT YANG DIRANCANG

No.	Parameter	Penelitian sebelumnya		Alat yang dirancang
		Ikhwan	Heri	
1.	Protokol VPN	SSTP	L2TP	PPTP
2.	*Router* yang digunakan	MikroTik	MikroTik	MikroTik
3.	OS komputer *client*	Windows 7	Windows 8	Windows 7
4.	Media konfigurasi VPN	WebFig/ Browser	WinBox	WinBox

III. METODE PENELITIAN

A. Topologi Jaringan

Topologi *Virtual Private Network* yang dirancang dapat dilihat pada Gbr 1. Komputer 1 merupakan perangkat yang akan di-*remote* dan memiliki alamat IP 192.168.88.254 yang diberikan oleh *router* MikroTik. Perangkat *Router* MikroTik difungsikan sebagai VPN Server. Komputer 1 terhubung ke *port ether* 2 *router* MikroTik menggunakan kabel UTP tipe *straight*. Alamat IP pada *port ether* 2 menggunakan alamat IP *default router* MikroTik, yaitu 192.168.88.1. *Port ether* 1 *router* MikroTik terhubung pada layanan internet dari ISP yang memiliki IP publik 103.83.174.25. Komputer 2 dijadikan sebagai VPN *Client* yang akan terkoneksi dengan VPN Server. Alamat IP dari komputer 2 berasal dari VPN Server, yaitu 192.168.88.10. Komputer 2 terhubung dengan internet menggunakan koneksi *Wi-Fi*. Protokol VPN yang digunakan adalah *Point-to-Point Tunneling Protocol* (PPTP).



Gambar. 1 Topologi Jaringan VPN

B. Perangkat Keras

Dalam artikel ini, digunakan 3 jenis perangkat keras yang digunakan, antara lain:

1. *Router* MikroTik hAP *lite* RB941-2nd
2. Kabel UTP tipe *straight* dengan konektor RJ45
3. Dua buah komputer dengan spesifikasi pada Tabel II

TABEL II
SPESIFIKASI KOMPUTER 1 DAN KOMPUTER 2

Spesifikasi	Komputer 1	Komputer 2
Prosesor	Intel *Core* i3 7020U	AMD *Dual-Core* C-50
RAM	12 GB	1 GB
Hard disk	1 TB	320 GB
Operating System	Windows 10	Windows 7

C. Perangkat Lunak

Terdapat dua buah perangkat lunak yang digunakan dalam artikel ini, antara lain:

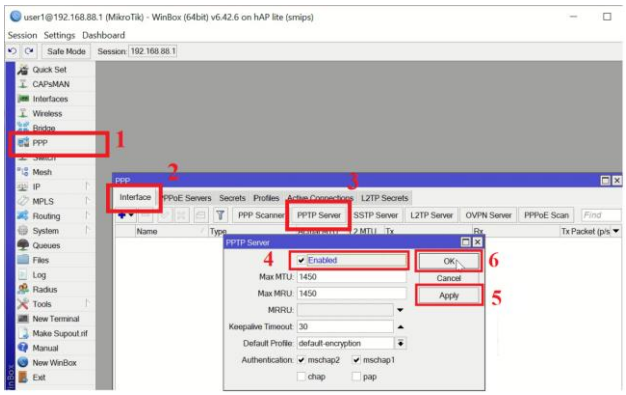
1. WinBox versi 3.27 (64-bit)
2. *Command Prompt* (CMD)

D. Konfigurasi VPN Server

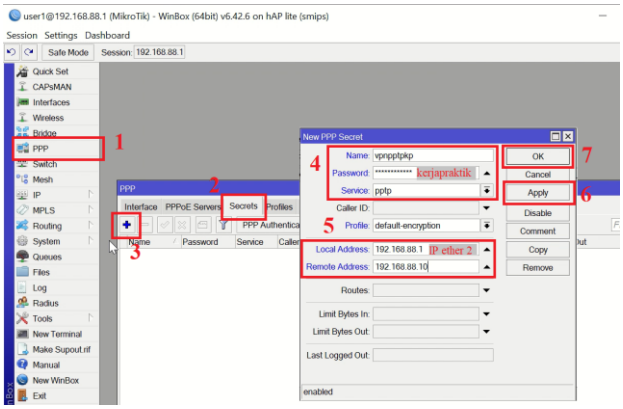
Perancangan yang dilakukan menjadikan *router* MikroTik sebagai VPN Server, oleh karena itu diperlukan beberapa konfigurasi pada menu PPP, yaitu mengaktifkan PPTP Server & membuat akun VPN dan pada menu *Firewall*, yaitu menambahkan *firewall rules* baru.

1. PPP

Mengaktifkan PPTP Server akan menjadikan *router* MikroTik sebagai VPN Server yang menggunakan protokol PPTP. Konfigurasi dimulai dengan memilih menu PPP → *Interface* → PPTP Server. Setelah kotak dialog PPTP Server muncul, klik *Enabled* → *Apply* → Ok. Konfigurasi pengaktifan PPTP Server dapat dilihat pada Gbr 2. Setelah PPTP Server diaktifkan, maka langkah selanjutnya adalah membuat akun VPN yang akan digunakan oleh VPN *Client* untuk dapat mengakses jaringan VPN yang dirancang. Pilih menu PPP → *Secrets* → + (menambah akun baru). Pada kotak dialog New PPP Secret, konfigurasi dilakukan sesuai pada Gbr 3. Nama akun VPN adalah "vpnpptpkp" dengan *password* "kerjapraktik". *Local address* diisi dengan alamat IP dari *port ether* 2 *router* MikroTik, yaitu 192.168.88.1, sedangkan *Remote address* diisikan alamat IP yang unik yang nantinya akan digunakan oleh VPN *Client*, yaitu 192.168.88.10.



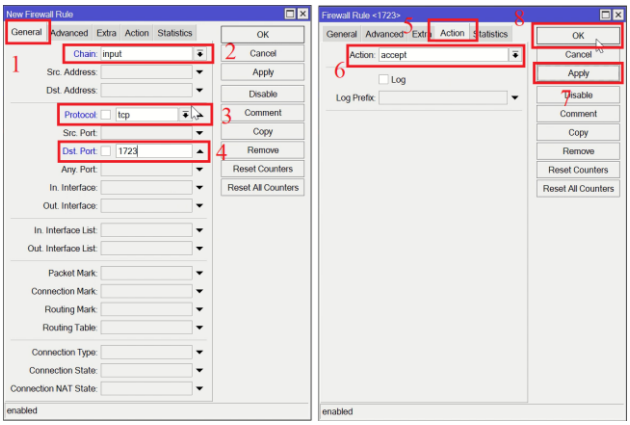
Gambar. 2 Konfigurasi PPTP Server



Gambar. 3 Konfigurasi Akun VPN

2. *Firewall*

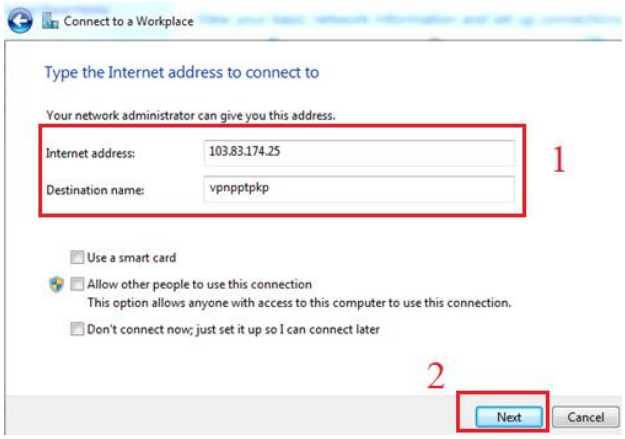
Protokol PPTP menggunakan protokol TCP 1723, oleh karena itu untuk dapat mengaktifkan VPN *tunnel* antara komputer yang memiliki *firewall*, perlu ditambahkan *firewall rules* pada *router* MikroTik yang mengizinkan protokol TCP *port* 1723. Menu *firewall* dapat diakses pada menu IP. Konfigurasi yang dilakukan untuk menambahkan *firewall rules* yang mengizinkan protokol TCP *port* 1723 dapat dilihat pada Gbr 4.



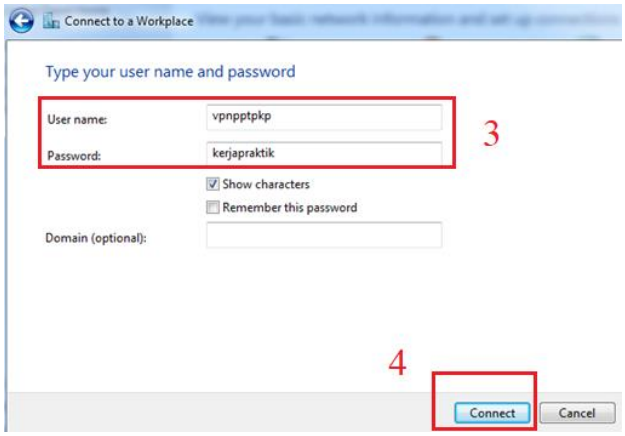
Gambar. 4 Konfigurasi Penambahan *Firewall Rules* Baru

E. Konfigurasi VPN Client

Konfigurasi yang dilakukan pada komputer *client* agar dapat terhubung dengan VPN adalah dengan memasukkan akun VPN dan komputer *client* harus terhubung dengan internet. Komputer *client* menggunakan sistem operasi Windows 7. Penambahan VPN pada Windows 7 dilakukan pada menu *Control Panel* → *Network and Sharing Center* → *Set up a new connection or network* → *Connect a workplace* → U*se my internet connectio*n (VPN). Setelah muncul kotak dialog *connect to a workplace*, konfigurasi dilakukan sesuai Gbr 5 dan Gbr 6. *Internet address* pada Gbr 5 diisikan dengan alamat IP publik pada *router* MikroTik, yaitu 103.83.174.25 sedangkan *destination name* diisikan "vpnpptpkp". Pada Gbr 6, *username* dan *password* diisikan sesuai dengan akun VPN yang dibuat pada VPN Server.



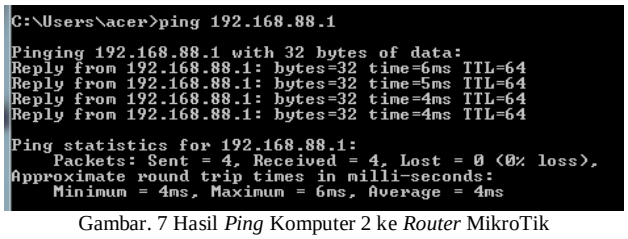
Gambar. 5 Konfigurasi IP Publik VPN



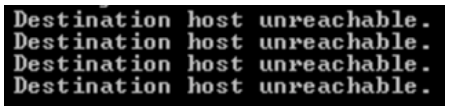
Gambar. 6 Konfigurasi Akun VPN

IV. HASIL DAN PEMBAHASAN

Pengujian dilakukan untuk mengetahui apakah komputer 2 telah terhubung dengan router MikroTik dan komputer 1 melalui jaringan VPN. Pengujian dilakukan dengan menjalankan perintah *ping* pada CMD melalui komputer 2 dan komputer 1. Perintah *ping* dari komputer 2 ditujukan ke alamat IP *router* MikroTik 192.168.88.1 dan alamat IP komputer 1 192.168.88.254. Gbr 7 menunjukkan hasil uji komputer 2 melakukan perintah *ping* ke *router* MikroTik sedangkan Gbr 8 menunjukkan hasil uji komputer 2 melakukan *ping* ke komputer 1.

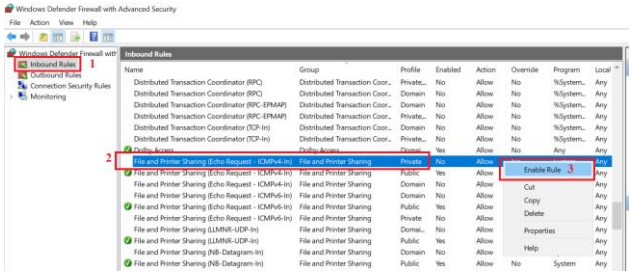


Gambar. 7 Hasil *Ping* Komputer 2 ke *Router* MikroTik



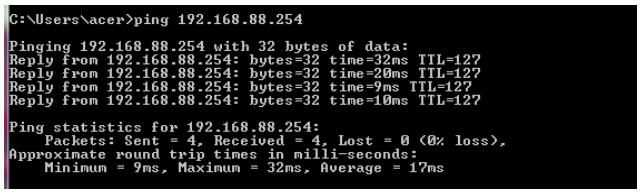
Gambar. 8 Hasil Uji *Ping* Komputer 2 ke Komputer 1

Hasil uji *ping* komputer 2 ke komputer 1 pada Gbr 8 menunjukkan bahwa *destination host unreachable.* Hal ini disebabkan karena, secara *default*, *firewall* sistem operasi Windows 10 pada komputer 1 tidak mengizinkan komputer lain yang berada dalam satu jaringan melakukan perintah *ping* demi alasan keamanan. Agar komputer 2 dapat melalukan *ping* ke komputer 1, *firewall* pada komputer 1 harus dikonfigurasi dengan mengaktifkan aturan *File and Printer Sharing* (*Echo Request* ICMPv4-*In*). Hal yang harus dilakukan adalah membuka *Advanced settings* pada *Windows Defender Firewall* → klik *Inbound Rules* → klik kanan pada aturan *File and Printer Sharing* (*Echo Request* ICMPv4-*In*) → klik *Enable Rule*. Gbr 9 menunjukkan konfigurasi untuk mengaktifkan aturan *File and Printer Sharing* (*Echo Request* ICMPv4-*In*).



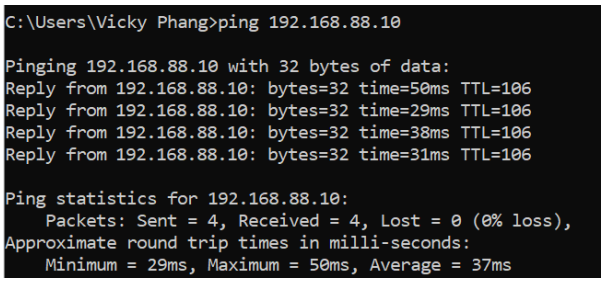
Gambar. 9 Konfigurasi Pengaktifan Aturan *File and Printer Sharing (Echo Request ICMPv4-In)*

Setelah mengaktifkan *File and Printer Sharing* (*Echo Request* ICMPv4-*In*), dilakukan pengujian kembali dan hasil uji *ping* komputer 2 ke komputer 1 dapat dilihat pada Gbr 10.



Gambar. 10 Hasil Uji *Ping* Komputer 2 ke Komputer 1 Setelah Konfigurasi *Firewall*

Pengujian selanjutnya dilakukan dengan menjalankan perintah *ping* dari komputer 1 ke alamat IP komputer 2, yaitu 192.168.88.10. Gbr 11 menunjukkan hasil uji *ping* dari komputer 1 ke komputer 2.



Gambar. 11 Hasil Uji *Ping* Komputer 1 ke Komputer 2

V. KESIMPULAN

Berdasarkan perancangan *virtual private network* dengan protokol PPTP menggunakan MikroTik, maka dapat diambil beberapa kesimpulan, antara lain:

1. Perancangan *virtual private network* dengan protokol PPTP menggunakan MikroTik berhasil menghubungkan komputer 2 yang berada di luar jaringan lokal dengan komputer 1 yang berada dalam jaringan lokal. Hal ini ditunjukkan hasil uji pada Gbr 10 dan Gbr 11.
2. Berdasarkan pengujian *ping* dari komputer 2 ke komputer 1 pada bab IV, aturan *File and Printer Sharing* (*Echo Request* ICMPv4-*In*) pada *firewall* bawaan Windows 10 komputer 1 harus diaktifkan, agar komputer 2 dapat melakukan *ping* ke komputer 1 melalui CMD.

Saran yang dapat diberikan untuk pengembangan perancangan *virtual private network*, antara lain:

1. Jika terdapat lebih dari satu komputer yang terhubung ke *router*, maka dapat dipertimbangkan untuk menggunakan perangkat *switch* untuk menghubungkan komputer tersebut.
2. Menggunakan koneksi internet dengan kecepatan yang stabil untuk menunjang keberlangsungan jaringan VPN.
3. Mempertimbangkan penggunaan protokol OpenVPN dan IKEv2 untuk keamanan yang lebih baik.

DAFTAR PUSTAKA

[1] Hafshah, S. Addy, dan M. K. Dyna, "Pendeteksi Gangguan Jaringan Lokal Menggunakan Metode Certainty Factor," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 13, no. 2, hal. 60–64, 2019.

[2] S. Hidayatulloh dan E. Rahmawati, "Perancangan Virtual Private Network Point to Point Berbasis Mikrotik," *Tek. Inform. STMIK ANTAR BANGSA*, vol. 4, no. 2, hal. 165–170, 2018.

[3] A. Fadlil, I. Riadi, dan S. Aji, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, hal. 11–19, 2017.

[4] W. O. Zamalia, L. M. F. Aksara, dan M. Yamin, "Analisis Perbandingan Performa Qos, Pptp, L2Tp, Sstp Dan Ipsec Pada Jaringan Vpn Menggunakan Mikrotik," *semanTIK*, vol. 4, no. 2, hal. 29–36, 2018.

[5] I. Ruslianto dan U. Ristian, "Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura," *Comput. Eng. Sci. Syst.*, vol. 4, no. 1, hal. 74–77, 2019.

[6] S. Heri Oky, "Perancangan Jaringan Virtual Private Network Menggunakan Mikrotik RB951 Pada Satuan Brimob Polda Jawa Timur," Surabaya, 2015.