# Metode *Point to Point Tunneling Protocol* Untuk Keamanan Jaringan Studi Kasus Kantor Walikota Administrasi Jakarta Barat

Fajar Akbar<sup>1</sup>, Susafa'ati<sup>2</sup>, Musriatun Napiah<sup>3</sup>

<sup>1,2,3</sup> Program Studi Teknik Informatika <u>1fajar.fkb@nusamandiri.ac.id,</u><sup>2</sup>susafa'ati.suf@nusamandiri.ac.id,<sup>3</sup>musnaf2015@gmail.com

Diterima	Direvisi	Disetujui
13-12-2019	15-12-2019	17-12-2019

Abstrak-Kemajuan dan perkembangan Ilmu Pengetahuan dan Teknologi saat ini sangatlah pesat, tentunya Sistem Keamanan Jaringan pun semakin berkembang seiring dengan kedua hal tersebut. Perusahaan – perusahaan sudah melakukan komputerisasi, sehingga setiap bagiannya menggunakan komputer dalam setiap operasionalnya, semakin maju dan berkembang perusahaan tersebut akan membuka cabang baru dalam operasionalnya baik di luar kota, negeri, ataupun benua untuk meningkatkan kualitas dan kuantitas produksi perusahaan. Dalam bidang administrasi pemerintah penting dalam manajemen pembagian jaringan, dan pertukaran data agar cepat, mudah, dan tepat dalam pengerjaannya, dan tidak mudah diakses pihak luar suku dinas kepemerintahan. Sistem keamanan jaringan yang baik, sangat diperlukan dalam pertukaran data dari kantor pusat ke kantor cabang sehingga dapat dilakukan secara aman dan terjamin dari pihak luar. Ada berbagai macam software aplikasi yang bisa digunakan dalam hal keamanan pada suatu jaringan, akan tetapi tidak semua software terjaga keamanan datanya dalam proses pertukaran data. Oleh karena itu dengan metode *point to point tunneling protocol* pada VPN sangatlah cocok jika digunakan dalam pertukaran data antar perusahaan karena metode ini menggunakan jalur *private* dengan ip *public* dalam pertukaran datanya, sehingga keamanan dalam hal kebocoran data sangat terjamin dari pihak luar yang tidak bertanggung jawab.

# Kata Kunci: *Point to Point Tunneling Protocol, VPN*, Sistem Keamanan Jaringan dan Kantor Administrasi Walikota Jakarta Barat

## PENDAHULUAN

Pada era globalisasi zaman sekarang, kemajuan dan perkembangan dunia teknologi dan internet sangatlah pesat sehingga berdampak di setiap aktivitas perusahaan, instansi atau lainnya, sebagai kebutuhan pokok dalam media komunikasi antar cabang perusahaan kantor pusat atau sebagai media dalam pertukaran data (sharing) antar cabang yang dapat diakses melalui jaringan komputer. Aktivitas aktivitas tersebut tentulah sangat beresiko apabila informasi yang penting dan berharga dapat diakses oleh pihak yang tidak berkepentingan. Keamanan suatu jaringan pada suatu perusahaan sangatlah penting dalam pertukaran data antar server dan client, misalkan dari kantor pusat server dengan kantor cabang *client*. Suatu perusahaan yang memiliki kantor cabang di berbagai daerah, kota, atau bahkan antar Negara diperlukan teknologi yang dan terpusat dalam pertukaran data aman perusahaan, begitupun halnya pada Kantor Walikota Administrasi Jakarta Barat mempunyai dua gedung yakni gedung Server dan gedung Client sehingga memerlukan teknologi keamanan pada pertukaran informasi. Data akan tersimpan di server terpusat dan akan diakses oleh client antar cabang perusahaan tersebut.

Sistem Jaringan yang aman pada Kantor Walikota Administrasi Jakarta Barat untuk mengatasi hal ini adalah dengan Menerapkan VPN (*Virtual Private Network*) dimana bisa menghubungkan dua perusahaan yang berbeda gedung sehingga dapat saling terkoneksi, begitupun kurangnya SDM (Sumber Daya Manusia) pada bagian Sudin Kominfo di Kantor Walikota Administrasi Jakarta Barat dalam menangani permasalahan yang terjadi dalam jaringan. Keamanan data dan *enkripsi* data dalam teknologi VPN adalah sebagai standar utama dalam penerapannya dengan menyertakan fitur utama yaitu *enkripsi* dan *tunneling*.

Menurut (Putra, Luthfi, & Yeni, 2018)Metode РРТР merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client (client yang berada jauh dari server) ke server pribadi perusahaan dengan membuat sebuah VPN (Virtual Private Network) melalui jaringan data berbasis TCP/IP. Protokol ini dikembangkan oleh Microsoft dan Cisco. Teknologi jaringan PPTP merupakan pengembangan dari remote access Pointto-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). Dari hasil penelitian di atas, penulis akan membahas pengamanan yang harus diterapkan pada Kantor Walikota Administrasi Jakarta Barat agar keamanan data dapat terjaga dalam pengaksesan, meminimalisir kurangnya SDM (Sumber Daya Manusia) dalam penanganan permasalahan yang terjadi agar cepat teratasi

#### METODE PENELITIAN

Teknik pengumpulan data yang digunakan oleh penulis dalam melakukan pengumpulan data dengan menggunakan metode sebagai berikut:

#### 1. Metode Observasi

Observasi atau pengamatan merupakan salah satu teknik pengumpulan data atau fakta. Disini penulis melakukan observasi dengan mengamati secara langsung untuk mendapatkan data-data tentang analisa jaringan komputer dan konfigurasinya pada Kantor Walikota Administrasi Jakarta Barat.

#### 2. Studi Pustaka

Dalam metode ini, pengumpulan data dilakukan dengan bersumber pada buku pegangan, Jurnaljurnal ilmiah, catatan-catatan kuliah dan buku-buku lain yang ada kaitannya dengan pengumpulan data yang penulis butuhkan sebagai bahan perlengkapan analisa perbandingan penulis.

## HASIL DAN PEMBAHASAN

## 1. Jaringan Komputer

Jaringan Komputer adalah hubungan antar dua komputer atau lebih dalam bentuk implementasi dan komunikasi data. Sebagaimana prinsipdasar dalam komunikasi data bahwa data yang dikirim harus diterima oleh komputer yang dituju dalam waktu yang secepatnya (Pratama;Marlinda, 2015)

## 2. Tunneling

Teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber tujuannya. Teknologi ini dibuat dalam pelaksanaannya dengan melintasi jalur umum namun tidak mempedulikan data milik orang lain yang sama-sama melintasi jalur tersebut, tetapi koneksi hanya melayani transportasi data dari pembuatnya (Mufida et al., 2018)

## 3. PPTP (Point to Point Tunneling Protokol)

Protocol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Keunggulan utama dari PPTP adalah memberikan keamanan serta *enkripsi* komunikasi melalui PTSN (*Public Switched Telephone Network*) ataupun Internet (Mufida et al., 2018)

#### 4. Topologi

Untuk topologi jaringan penulis mengusulkan agar tetap menggunakan topologi yang sudah ada karena sangat tepat diterapkan pada Kantor Walikota Administrasi Jakarta Barat baik pada gedung *server* maupun pada gedung *client*.

## 5. Skema Jaringan

Untuk skema jaringan tetap menggunakan skema yang sudah berjalan hanya saja penulis menambahkan satu buah *server* untuk VPN dengan menggunakan metode *point to point tunneling protocol* baik itu pada gedung *server* maupun pada gedung *client*, sehingga kedua jaringan tersebut dapat saling terhubung, karena disini menggunakan topologi star maka tidak akan mengganggu kinerja jaringan yang sedang berjalan.



Sumber : peneltian (2019) Gambar 1. Skema Jaringan Usulan Gedung *Server* 



Sumber : penelitian (2019) Gambar 2. Skema Jaringan Usulan Gedung *Client* 

#### 6. Keamanan Jaringan

Keamanan yang diterpakan pada gedung *server* dan gedung *client* bertumpu pada PC *Router*, Sedangkan untuk *client* menggunakan antivirus pada masing-masing PC.

## 7. Antivirus

Berfungsi untuk mencegah penyebaran *virus* yang datang dari *client* pada jaringan tersebut. Antivirus ini akan memberikan perlindungan dan keamanan pada data dan system yang ada pada komputer.

#### 8. VPN (Virtual Private Network)

Teknologi komunikasi pada sebuah jaringan yang memudahkan untuk berkomunikasi antara jaringan publik dengan jaringan lokal. VPN biasanya digunakan untuk menghubungkan jaringan antar tempat yang berjauhan, seperti halnya antara kantor pusat dengan kantor cabang. Dengan cara tersebut maka setiap jaringan akan mendapatkan hak yang sama dan pengaturan yang sama seperti halnya berada dalam jaringan atau *network* itu sendiri (Mufida, Irawan, & Chrisnawati, 2018)

Sistem keamanan jaringan menggunakan VPN dengan metode *point to point tunneling protocol* dapat mencegah kehilangan data ke pihak luar yang tidak bertanggung jawab, karena *tunneling* menggunakan jaringan *private* sehigga kerahasiaan data dapat terjaga dari pihak luar baik di gedung *server* maupun di gedung *client*.

#### 9. Rancangan Aplikasi

Untuk perancangan aplikasi penulis merapkan system keamanan dengan metode *point to point tunneling protocol* pada VPN dengan menggunakan mikrotik OS. Penulis melakukan konfigurasi pada beberapa *Ethernet*, seperti *Ethernet* untuk ip *public*, ip *local*, *DNS*, *dll*. Setelah melakukan konfigurasi penulis *login* pada *winbox* dengan menggunakan *ip public*. Dan berikutnya melakukan konfigurasi untuk ip *address* sampai dengan konfigurasi untuk VPN dengan metode *point to point tunneling protocol*. Hasil akhir dari konfigurasi dapat dilihat pada pegujian awal dan pengujian akhir.

Pada bagian manajemen jaringan penulis membahas jaringan usulan untuk diterapkan pada Kantor Walikota Administrasi Jakarta Barat. Manajemen jaringan yang penulis usulkan yakni berhubungan dengan sistem keamanan jaringan menggunakan *point to point tunneling protocol.* 

#### 10. Pengujian Jaringan

Pada bagian pengujian jaringan, penulis akan membahas proses pengujian dari sebelum dilakukan konfigurasi VPN dengan metode *point to point tunneling protocol* sampai dengan telah dilakukan konfigurasi VPN.

#### a. Pengujian Jaringan Awal

Pengujian ini dilakukan sebelum adanya konfigurasi *point to point tunneling protocol* pada komputer *server* dan komputer *client*, bisa kita lakukan dengan tes koneksi PING.



Sumber : Penelitian (2019)

Gambar 3. Tes ping komputer *server* ke komputer client

dimana pengujian ini adalah sebelum adanya kofigurasi PPTP antar gedung *server* dengan gedung *client*, masih dalam kondisi RTO (*Request Time Out*) yang artinya masing-masing *sever* yang ada di kedua gedung belum saling terkoneksi dalam jaringan VPN.

#### b. Pengujian Jaringan Akhir

Untuk tahap pengujian akhir disini penulis akan menjelelaskan mulai dari installasi mikrotik OS, pemberian IP *Address*, IP *Route Gateway*, IP DNS, dan PPTP *Client*, sampai berhasil atau tidaknya konfigurasi tersebut.

Pada bagian jendela *winbox*, lakukan login dengan menggunakan IP *Public*, dapat dilihat pada gambar di bawah ini:



Sumber : Penelitian (2019) Gambar 5. Login Winbox

Selanjutnya klik pada bagian IP Address kemudian pilih "connect" untuk masuk ke bagian konfigursi dengan menggunakan winbox.

Lakukan konfigurasi IP *Gateway*. Disini gateway merupakan penghubung pada sebuah jaringan komputer lainnya sehingga memudahkan dalam akses informasi.

Masuk ke menu IP > *Route* > *Gateway* > 192.168.43.1 > *apply* > *ok* 

Gatareay         10:168.0.1         reschable vlan:1         Reno           Orek Gereys	Dst. Address:	0.0.0.0/0		Copy
Oreck Gateway	Gateway	192.168.43.1	reachable wan1	Remov
Type uncat Distance [ Sope 30 Type Sope 10 Rodrog Marc	Check Gateway:			
Datases         1           Segregation         30           Trade Source         10           Routing Mate         1	Type:	unicast		
Scope (30 Target Scope (10 Roung Mark	Distance:	1		
Target Scope: 10 Roung Mark:	Scope:	30		
Routing Mark:	Target Scope:	10		
	Routing Mark:			
Pref. Source:	Pref. Source:			

Sumber : Penelitian (2019)

Gambar 6. Konfigurasi IP Gateway

Lakukan konfigurasi IP DNS Klik menu IP > DNS > *Servers* = 192.168.137.1, 8.8.8.8 > centang  $(\boxdot)$  pada bagian *allow-remote-request* > *apply* > lalu pilih ok



Sumber : Penelitian, 2019 Gambar 7. Konfigurasi IP DNS

Lakukan konfigurasi *firewall* untuk bagian NAT, Pilih menu IP > *Firewall* > *NAT* > + > *chain* > pilih *srcnat* > *out-interface* > *ether1* 

NAT Rule						
General	Advanced	Extra	Action	Statistic		ок
	Chain: 📗	connet				Cancel
Sro	Address:				-	Apply
Det	Address:				-	Disable
	Protocol:				-	Comment
	Src. Port:				-	Сору
	Det. Port:				-	Remove
	Any Port:				-	Reset Counters
In.	Interface:				-	Reset All Counter
Out	Interface:	wian	E.		<b>Ŧ</b> ~	
In. Inte	aface List:				-	
Out: Inte	rface List:				-	
Pac	ket Mark:				-	
Connec	tion Mark:				-	
Rou	ting Mark:				-	
Rout	ing Table:				-	
Conneg	tion Time!				-	



Kemudian pada bagian tab "action" kita pilih masquerade



Sumber : Penelitian (2019) Gambar 9. Konfigurasi IP *Firewall* 

Lakukan konfigurasi yang sama untuk *Router* dan gedung *server* pada gedung *client*.

## c. Konfigurasi PPTP Server

Selanjutnya setelah kita melakukan konfigurasi dasar untuk masing-masing *Router*, kita akan melakukan konfigurasi untuk PPTP *Server* sesuai dengan skema jaringan usulan yang telah penulis gambarkan, maka kita akan melakukan konfigurasi PPTP *Server* pada gedung *server*.

Aktifkan PPTP Server, klik PPP > pilih PPTP Server > centang ( $\square$ ) pada bagian *enabled* > apply > ok.

+• = 🖉 🕺	67	PPP Scanner	PPTP Server	SSTP Sen
PPTP Server				
	<ul> <li>Enabled</li> </ul>			ОК
Max MTU:	1450			Cancel
Max MRU:	1450			Apply
MRRU:			•	
Keepalive Timeout:	30			
Default Profile:	default-encryptic	on	Ŧ	

Sumber : Penelitian, 2019

Gambar 10. Konfigurasi PPTP Server

Disini kita akan menggunakan IP Pool untuk membuat PPTP.

Masuk ke menu IP > Pool > Klik + > isikan "name" dan "range" IP Address > pada kolom address.

+ - 7	
IP Pool <ppp></ppp>	
Name: ppp	ок
Addresses: 192.168.100.2-192 🗢	Cancel
Next Pool: none 두 🔺	Apply
	Сору
	Remove

Sumber : Penelitian (2019)

Gambar 11. Konfigurasi IP Pool

d. Konfigurasi untuk VPN Server

Masuk ke menu PPP > Klik tab *profiles* > tambahkan *profile* baru dengan mengklik "+" masukan data sebagai berikut:

Name: nama profilenya Local Address: IP Address van

Local Address: IP Address yang diberikan untuk VPN Servernya

Remote Address: pilih nama ip pool yang tadi dibuat

jika sudak klik ok





Gambar 12. Konfigurasi Profile VPN

Pembuatan *user* baru pada PPTP, Klik pada menu PPP > pilih *Secrets* > + > lalu isikan: *Username & Password:* untuk proses *autentikasi client* yang akan terkoneksi ke PPTP *Server*, penggunaan huruf besar dan huruf kecil akan berpengaruh.

Local Address: alamat IP yang akan terpasang pada router itu sendiri (PPTP Server) setelah link PPTP terbentuk

*Remote Address:* Alamat IP yang akan diberikan *Client* setelah link PPTP terbentuk utuk "*Profile*" pilih *profile* yang sebelumnya sudah dibuat kemudian apply > ok

nterface PPPoE	Servers Secre	Profiles	Active Connec
+ >		PPP Auth	entication&Acco
PPP Secret <pptp< td=""><td></td><td></td><td></td></pptp<>			
Name:	PPTP		ок
Password:			Cancel
Service	pptp		Apply
Caller ID:		-	Disable
Profile	pptp_skripsi		Comment
Local Address:	5	-	Сору
Remote Address:	C.	-	Remove
Routes:	C	-	
Limit Bytes In:	6	-	
Limit Bytes Out:	ſ	-	
Last Logged Out:	Jul/12/2019 17	:58:43	



Sampai disini untuk konfigurasi *router* PPTP Server sudah selesai, selanjutnya kita lakukan konfigurasi untuk sisi *client*.

Tambahkan *interface* baru PPTP *Client* Klik pada menu PPP > + > PPTP *Client* 



Sumber : Penelitian (2019) Gambar 14. Interface PPTP Client

Lakukan *Dial Out* ke IP *Public Router* A (PPTP *Server*), masukan *username* dan *password* sesuai dengan pengaturan *secret* PPTP *Server* 

		PPP Scanner	PPTP Server	SSTP
New Interface				
General Dial Out Stat	us Traffic			OK
Connect To:	172.168.10.1	10		Cancel
User	PPTP			Apply
Password:			-	Disable
Profile:	pptp_skripsi		•	Commen
Keepalive Timeout:	60		-	Сору
	Dial On D	emand		Remove
	Add Defa	ult Route		Torch
Default Route Distance:	0			
Allow:	l⊯ mschap2 I⊮ chap	l⊻ machap1 I¥ pap		
(contract T			Status	



Setelah koneksi PPTP terbentuk, akan muncul IP Address baru di kedua Router

Selanjutnya konfigurasi untuk ARP, klik menu *interface* > pilih *ether2* > klik tab *general* > ARP > *proxy* - *arp* > *apply* > *ok* 

DR	Name ++ costs-PPTP-1>	Interface cether2>	STATUL INTATIL TO		D.
DR	+++optp-PPTP>	General Ethemet Loop	Protect Overall Rats Rk Stats		OK
R	4l+ether2	Name	hittan2		Cancel
	+t+other4	Type:	Ethemet		Book
8	We wiam 1	MTU:	1500		1009
		Actual MTU:	1500		Disable
		L2 MTU:	1598		Comment
		Max 12 MTU	2028		Terch
		MAC Address	CC:20 E0:60-C5 7F		Cable Test
		ARP	proxy-arp	141	Blink
		ARP Timeout		*	Reset MAC Add
				Tran 1	Reset Counte
		Master Port:	none		
		Bandwidth (Rk/Tx):	unlimited   ¥ / unlimited		
		Swech:	ewtch1		

Sumber : Penelitian (2019)

## Gambar 16. Konfigurasi ARP

## e. Membangun VPN

Lakukan penyettingan untuk VPN Server pada winbox, Pastikan laptop sudah terkoneksi dengan internet.

Buka *control panel* pada pc, kemudian pilih menu *open network and sharing center*, kemudian *create* koneksu baru dengan memilih *set up new connection or network*\_\_\_\_\_

194	ton removing security
10	Set up a new connection or network
*	Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point
10	Connect to a network
~	Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
ađ,	Choose homegroup and sharing options
	Access files and printers located on other network computers, or change sharing settings.
	Troubleshost problems
-	Diagnose and repair network problems, or get troubleshooting information.

## Sumber : Penelitian (2019) Gambar 17. Konfigurasi VPN Server

Pada tampilan *windows* selanjutnya, pilih connect to a workplace, lalu klik next



Sumber : Penelitian (2019)

Gambar 18. Konfigurasi VPN Server

Pada langkah berikutnya kita akan diminta untuk memasukan IP Address yang akan melakukan koneksi yaitu IP Address public router A, Destination name adalah parameter untuk memberikan nama pada interface VPN yang sudah dibuat.

Non-strates defautions (action by optimizes Defaution defautions)  Provide a strategy (action defautions)  Provide a strateg		Net Can
War cherron de management or cup or pay of a defaults.     Access and a default of a defaul	Don't connect no	wr, just set it up so I can connect later
Ver refreed Annihuster com yer yer ye al editoria. Desimated Annie VPH Connection Desimated Annihuster VPH Connection Desimated Annihuster A	2 Allow other peop This option allow	le to use this connection is anyone with access to this computer to use this connection.
Verun netiveek administrateri cun piley you triis adeletes. Internet address. Destination name VPN Cennestian	Oue a umart card	
Vou network administration con give you truth address. Internet address. Destination name: VPM Convestion		
Your network administrator can give you this address. Internet address: 172.168.10.10		VPN Connection
Your network administrator can give you this address.	Dectination name	
	Internet address Dedination name:	172.168.10.10
Type the threather address to connect to	Your network administra Internet address: Destination name:	tor can give you this address. 172.168.10.10

Sumber : Penelitian (2019) Gambar 19. Konfigurasi VPN Server

Selanjutnya masukan *username* dan *password* yang sudah dibuat tadi di konfigurasi PPTP

G in Construction	14.1		Constitution
Type your user sa	ime and password		Connecting to VPN Connection.
Denare 7axod	919 		\$Þ
Denimitytenit	Die beschn Einenster für passend		Verljing var name and personal.
		Lavet Lave 0	

Sumber : Penelitian (2019) Gambar 20. Koneksi VPN

Jika sudah selesai maka akan muncul *interface* baru sesuai dengan nama VPN *Connection* 



Sumber : Penelitian (2019) Gambar 21. Koneksi VPN

Tampilan hasil koneksi VPN dari server ke client yakni antar gedung server dan gedung client

Administrator: C:\Windows\system32\cmd.exe	×
Ping statistics for 172.168.10.10: Approximate reaction of the state of the stat	с Ш
C:\Users\Yubi>ipconfig	
PTP adapter UFN Connection: Connection-specific DMS Suffix : 1 192.169.100.9 Subnet Half	
Vireless LAN adapter Wireless Network Connection:	
Media State Media disconnected Connection-specific DNS Suffix . :	

Sumber : Penelitian (2019) Gambar 22. Hasil Koneksi VPN

Disini kita cek *ip address* yang di dapatkan si *client* setelah terkoneksi ke VPN, sesuai dengan IP Pool yang tekah kita tentukan di konfigurasi PPTP *Server* di atas, yaitu 192.168.100.10, selanjutnya kita tes koneksi ping ke *server*:



Sumber : Penelitian (2019) Gambar 23. Hasil Koneksi VPN

Berikut ini adalah tampilan pada PPTP Server ketika ada client yang terkoneksi pada VPN



Sumber : Penelitian (2019) Gambar 24. Tampilan PPTP Server

## KESIMPULAN

Dari pembahasan yang telah penulis jelaskan di atas mengenai peranan jaringan komputer dalam kehidupan sehari-hari, dengan ini penulis menarik kesimpulan bahwa dengan adanya keamanan penerapan jaringan komputer menggunakan metode PPTP (Point to point tunneling protocol) pada VPN memberikan suatu kemudahan bagi pihak pekerja IT dalam mengatasi permasalahan yang terjadi antar kantor yang berjauhan jaraknya, dan meberikan keamanan pada pengiriman data yang di transmisikan dengan metode enkripsi dalam jaringan private, sehingga sangat terjaga keamanannya dari pihak yang tidak beratanggung jawab.

## REFERENSI

- Mufida, E., Irawan, D., & Chrisnawati, G. (2018). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, *16*(2), 9. https://doi.org/10.30812/matrik.v16i2.7
- Pratama; Marlinda. (2015). Perancangan Jaringan Komputer Menggunakan Aplikasi Vhp Online Reporting System. *Teknik Komputer AMIK BSI*, 1(1), 106–113.
- Putra, J. L., Luthfi, I., & Yeni, A. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan. 3(2), 260–267.
- Mufida, E., Irawan, D., & Chrisnawati, G. (2018). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, *16*(2), 9. https://doi.org/10.30812/matrik.v16i2.7
- Pratama; Marlinda. (2015). Perancangan Jaringan Komputer Menggunakan Aplikasi Vhp Online Reporting System. *Teknik Komputer AMIK BSI*, 1(1), 106–113.
- Putra, J. L., Luthfi, I., & Yeni, A. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan. 3(2), 260–267.
- Mufida, E., Irawan, D., & Chrisnawati, G. (2018). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal*

*Matrik*, *16*(2), 9. https://doi.org/10.30812/matrik.v16i2.7

Pratama; Marlinda. (2015). Perancangan Jaringan Komputer Menggunakan Aplikasi Vhp Online Reporting System. *Teknik Komputer AMIK*  *BSI*, *1*(1), 106–113.

Putra, J. L., Luthfi, I., & Yeni, A. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan. 3(2), 260–267.