Vol 2 (2021) No 2

Jitsi Jurnal Ilmiah Teknologi Sistem Informasi

http://jurnal-itsi.org ISSN 2722-4619 (Print) ISSN 2722-4600 (Online)

# OpenVPN Server Menggunakan Ubuntu Server 20.04 LTS pada Amazon Web Services

Cilvia Chairunnisa[#], Indri Rahmayuni[#], Deddy Prayama[#]

[#] *Jurusan Teknologi Informasi, Politeknik Negeri Padang, Limau Manis, Padang, 25164, Indonesia*
*E-mail: rahmayuni@gmail.com, deddy@pnp.ac.id*

**ABSTRACTS**

Computer network is a technology that is widely used by companies that functions to connect one location to another. The use of the internet as a communication medium is not only very beneficial for the company, but still has weaknesses in terms of security. The obstacles faced are how to access data in the office and turn employee devices into a network required for API testing without having to come directly to the office, of course with a very adequate level of security. The solution that can be used for this problem is to build an OpenVPN server as a tunnel to be applied to help employees access the office network or other employees. By implementing the system, testing the API on mobile applications, which runs on the local office computer or runs on client computers or other employees.

**KATA KUNCI**

*OpenVPN,*
*API,*
*Tunnel,*
*Amazon Web Services,*
*Ubuntu Server*

**ABSTRAK**

Jaringan komputer merupakan satu teknologi yang banyak digunakan oleh perusahaan yang berfungsi menghubungkan satu lokasi dengan lokasi yang lainnya. Penggunaan internet sebagai suatu media komunikasi selain sangat bermanfaat untuk perusahaan, namun tetap memiliki kelemahan dalam hal keamanannya. Kendala yang dihadapi yaitu bagaimana mengakses data yang berada dikantor dan menjadikan perangkat karyawan menjadi satu jaringan yang diperlukan untuk testing API tanpa harus datang langsung ke kantor, tentunya dengan tingkat keamanan yang sangat memadai. Solusi yang bisa digunakan untuk masalah tersebut yaitu membangun sebuah sebuah server OpenVPN sebagai tunnel untuk diteraptakan agar dapat membantu karyawan untuk dapat mengakses jaringan kantor atau karyawan lainnya. Dengan mengimplementasikan sistem tersebut testing API pada aplikasi mobile, yang mana berjalan pada komputer local kantor maupun berjalan pada computer client atau karyawan lain.

## 1. PENDAHULUAN

Pemanfaaatan jaringan komputer untuk perusahaan sudah tidak dapat dipungkiri lagi untuk saat ini. Jaringan komputer memberikan kemampuan sebagai media komunikasi yang dapat mempercepat proses kerja baik dari segi waktu maupun ketepatan. Selain itu teknologi informasi dapat mempermudah dalam mengakses sebuah informasi. Perkembangan dunia teknologi informasi saat ini sudah sangat pesat khususnya internet, begitu banyak aktifitas manusia menjadi lebih cepat diselesaikan dengan adanya teknologi internet tersebut.

Pertukaran informasi dari satu tempat ke tempat lain menjadi mudah dan sangat cepat berkat adanya internet. Proses pertukaran data tersebut hanya membutuhkan beberapa detik untuk sampai ke tempat yang dituju. Kehandalan internet memungkinkan komunikasi yang tidak lagi terbatas oleh jarak dan waktu, menjadikan internet kian diminati. Internet sebagai suatu mediasi komunikasi selain sangat bermanfaat namun tetap memiliki kelemahan dalam keamanannya, terlebih sebagai media trasmisi data yang penting.

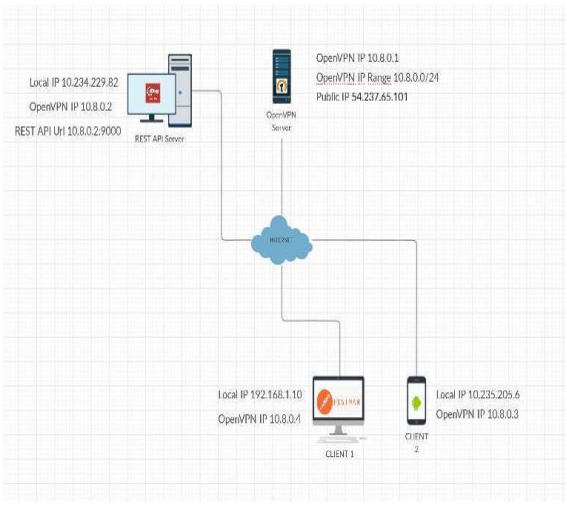
Salah satu upaya yang dilakukan adalah dengan membangun jaringan private pada layanaan jaringan publik atau sering disebut dengan Virtual Private Network. VPN (Virtual Private Network) merupakan suatu bentuk jaringan private yang melalui jaringan publik (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Hubungan ini dibangun melalui suatu tunnel (terowongan) virtual antara dua node. Dengan menggunakan jaringan publik ini, user dapat tergabung dalam jaringan local, mendapatkan hak dan pengaturan yang sama seperti ketika user berada di kantor [1].

## 2. METODOLOGI PENELITIAN

aktifitas manusia menjadi lebih mudah dengan adanya jaringan internet seperti proses mengirim data dari satu tempat ke tempat lain. Proses pengiriman data tersebut hanya membutuhkan beberapa detik untuk sampai ke tempat yang dituju. Tetapi dengan perkembangan jaringan internet tersebut banyak oknum yang mencoba memanfaatkan jaringan internet untuk mencuri data. teknologi atau sistem yang dapat mengamankan data pada saat proses pengiriman. Dengan menggunakan teknologi Virtual Private Network (VPN) dapat menjamin keaman dalam proses pengiriman data melalui jaringan internet.VPN (Virtual Private Network) adalah sebuah penghubung internet satu dengan internet dengan internet yang lain yang bersifat pribadi. Pada VPN terdiri dari enkripsi,autenikasi dan autorisasi. Enkripsi adalah sebuah proses pengubah data kedalam bentuk dapat yang bisa dibaca oleh penerima. Pesan yang telah dienkripsi dapat dibaca dengan cara menjalankan kunci dekripsi yang benar. Pada VPN terdapat sebuah Tunneling Protocols atau terowongan. Tunneling memiliki koneksi Point to Point yang bersifat connectionless. Protocol yang biasa digunakan yaitu, IPSec (IP Security), PPTP ( Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) dan SSL/TLS. IPSec merupakan standar keamanan jaringan transmisi dan autentikasi pengguna melalui jaringan public. IPSec beroperasi pada Network Layer dari tujuh OSI Layer (Open Sistem Interconnection Layer). OSI Layer merupakan system berkomunikasi dengan system lainnya yang bersifat terbuka.

Amazon Web Services (AWS) adalah salah satu penyedia layanan cloud computing selain dari Microsoft Azure, Google Cloud Platform, IBM Bluemix dan Hereku yang tepercaya dan aman. AWS menawarkan tenaga komputasi, ruangan penyimpanan dan fungsionalitas lainnya yang membantu banyak pebisnis untuk berkembang dan menjalankan aplikasi dengan baik. Salah satu kelebihan dari AWS adalah Banyak fitur layanan AWS yang bisa dipakai untuk membangun produk atau startup sesuai kebutuhan layanan, adapun kelemahan aws adalah belum dapat menanage resource suatu layanan AWS sehingga tagihan yang dibayarkan dalam jumlah yang besar ditiap bulan.

OpenVPN adalah sebuah aplikasi open-source untuk membuat VPN (Virtual Private Network) yang memiliki koneksi point-to-point pada tunnel yang telah ter- enkripsi. Untuk melakukan authentikasi menggunakan OpenVPN dibutuhkan private keys, certificate atau username-password untuk membangun sebuah koneksi. OpenVPN memiliki cara kerja server dan client memiliki jaringan internet yang tetap. Sebuah perusahaan memiliki router maka sebelum digunakan router tersebut dikonfigurasi firewall-nya untuk mencegah akses terhadap jaringan didalamnya dan dilakukan konfigurasi pada OpenVPN agar dapat melewati router. Aplikasi OpenVPN harus terpasang didalamnya, dan harus terkonfigurasi agar dapat terkoneksi. Data yang melewati OpenVPN dienkripsi telebih dahulu kemudian didekripsi sesudah transmisi. Enkripsi bertugas sebagai keamanan data sebuah terowongan (tunnel).



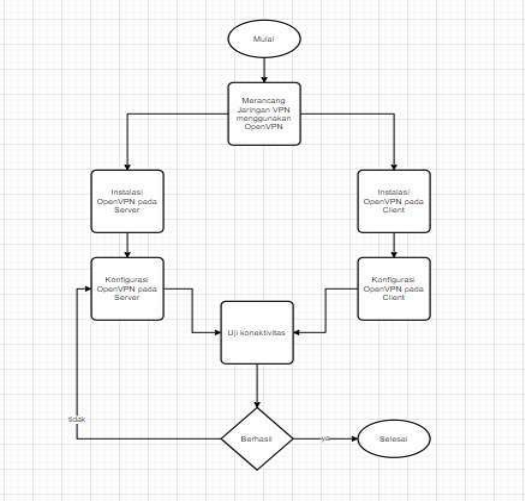

**GAMBAR 1.** Topologi Jaringan

Untuk membangun sebuah sistem pengujian REST API menggunakan OpenVPN dengan sistem operasi Linux Ubuntu 20.04 LTS dari layanan Koneksi OpenVPN dibuat antara dua akses internet dengan firewall. Aplikasi disetting agar dapat terhubung antara partner VPN dapat dilakukan. Firewall diatur agar bisa akses dan pertukaran data antara partner VPN yang telah aman sebelumnya karena telah dilakukan enkripsi. Key enkripsi dibuat sebanyak pengguna VPN agar pertukaran data dapat dilakukan oleh pengguna VPN yang telah diverifikasi. Amazon Web Services (AWS) diperlukan sebuah rancangan topologi jaringan seperti pada gambar 1.

Software yang digunakan dalam membuat sistem pengujian REST API menggunakan aplikasi OpenVPN, dan sistem ini juga menggunakan menggunakan servers AWS sebagai hosting serta platform untuk menginstal server Linux Ubuntu 20.04 LTS, meremote server yang telah dibuat menggunakan software Putty

Server yang digunakan dalam sistem ini adalah server AWS (Amazon Web Services). Server yang dibutuhkan sebagai berikut :

1. Sistem operasi yang digunakan untuk mengakses server atau Amazon Machine Image, yaitu Ubuntu Server 20.04 LTS
2. Tipe Instance yang digunakan, yaitu t2.micro dengan 1 vCPUs dan 1 GB RAM
3. Keamanan Grup (Security Group) yang digunakan untuk keamanan mengakses server: HTTP (Hypertext Transfer Protocol) port 80, SSH (Secure Shell) port 22, Custom UDP (User Data Protocol) port 1194, HTPPS (Hypertext Transfer Protocol Secure) port 443




**GAMBAR 2.** Kerja Sistem

Flowchart alur kerja sistem adalah algoritma dari jalannya sistem pengujian. Alurkerja sistem yang akan dibuat yaitu client akan diberikan akses kepada akses kepada server OpenVPN oleh host, Ketika client melakukan koneksi, OpenVPN akan memberikan ip kepada masing-masing client, client dapat terhubung ke jaringan yang sama dari lokasi yang berbeda, client juga bisa melakukan banyak kegiatan dengan jaringan tersebut, seperti remote antar client dengan client, atau client dengan host. Pada pembuatan tugas akhir ini, koneksi OpenVPN akan diimplementasikan sebagai tunnel untuk melakukan request API antar client. Alur kerja sistem dapat dilihat pada gambar 2.

## 3. HASIL DAN PEMBAHASAN

Setelah melakukan proses analisa dan perancangan maka langkah selanjutnya yaitu melakukan proses implementasi terhadap sistem yang dibangun. Dalam bab ini akan membahas tentang implementasi CI/CD Spring Java REST API dengan OpenVPN Server pada Ubuntu Server 20.04 LTS. Proses implementasi dimulai dengan membuat server di AWS (Amazon Web Service) dan melakukan proses instalasi serta konfigurasi tools yang digunakan.

### *3.1. Pembuatan Server*

OpenVPN Server dibuat menggunakan Ubuntu Server 20.04 LTS sebagai sistem operasi, dapat dilihat pada gambar 4.2. Perancangan server untuk OpenVPN ini menggunakan platform cloud komprehensif yaitu Amazon Web Services (AWS) dari perusahaan Amazon. Akses yang diberikan jurusan berupa akses student (pelajar), jadi layanan yang dapat di akses terbatas. Layanan yang di pakai adalah layanan Amazon Elastic Compute Cloud (Amazon EC2), instance type t2.micro, mempunyai 1 vCPUs, memory(GiB) 1, CPU. Security Group yang digunakan pada sistem ini adalah launch-wizard-2 yaitu yang berisikan Inbound rules HTTP(TCP) port 80,SSH(TCP) port 22, Costum UDP port 1194, HTPPS(TCP) 443,All IPv4 ICMP 0-65535. Berikut Langkah-langkahnya :

1. Masuk ke AWS dan Launch Instance
2. Pada tampilan Choose AMI Ubuntu Server 20.04 LTS
3. Melakukan Configure Security Group seperti tampilan dibawah ini, lalu Review and Launce
4. Pembuatan PuTTY Public Key
   Dalam perancangan server pada aws maka akan diberikan file dengan ekstensi .pem (Privacy Enchanted Mail) dengan nama file ubuntu.pem, lalu file tersebut diubah ke ekstensi .ppk (PuTTY Public Key) menggunakan software PuTTYGEN
5. Remote Server
   Software yang digunakan untuk meremote server AWS adalah PuTTY melalui protokol jaringan SSH (Secure Shell) dengan default port 22 melalui jaringan internet. Untuk meremote server diperlukan hostname atau ip address maka digunakan ip public server dengan port 22 dan connection type SSH. Lalu pilih menu SSH – Auth cari file dengan ekstensi PuTTY Public Key yang bernama ubuntu2.ppk.

*3.2. Konfigurasi Server dan Install Software*

Pada konfigurasi server dan instal software ini memiliki 2 tahapan yaitu Tahap Update dan Upgrade, dan install OpenVPN Server.

1. Tahap Update dan Upgrade

   Pada tahap ini akan dilakukan update dan upgrade server yang baru saja di buat. Update berfungsi untuk memperbaharui daftar paket yang tersedia di repository sekaligus memeriksa ada pembaruan versi paket yang tersedia untuk diunduh. Upgrade berfungsi menginstal versi terbaru dari semua paket saat ini yang diinstal pada sistem dari sumber-sumber yang disebutkan dalam /etc/apt/sources

   ```
   # apt update
   # apt upgrade
   ```

2. Tahap Install OpenVPN Sever

   Pada tahap ini merupakan tahap instalasi OpenVPN Server. OpenVPN merupakan aplikasi open-source untuk membuat Virtual Private Network (VPN) aplikasi yang dapat terkoneksi point- to-point tunnel yang telah terenkripsi. Proses install OpenVPN dilakukan dengan download openvpn-install.sh terlebih dahulu, lalu mengganti mode file tersebut agar bisa dieksekusi dengan menggunakan perintah chmod:

   ```
   # wget https://git.io/vpn -O openvpn-install.sh.
   # chmod +x openvpn-install.sh.
   ```

   Menjalankan openvpn-install.sh untuk instalasi OpenVPN server atau membuat konfigurasi untuk diberikan kepada client. Langkah pertama dalam membuat config adalah memasukan hosname atau ip public, yang mana ip public pada server yang di buat. Lalu untuk protocol yang digunakan adalah UDP. Menentukan port yang digunakan, yaitu 1194 yang telah dibuka terlebih dulu pada security group di AWS saat membuat server sebelumnya, kemudian memilih DNS server untuk client, DNS yang dipakai pada sistem ini. Setelah melakukan konfigurasi diatas, maka langkah selanjutnya adalah membuat nama file berekstensi .ovpn yang akan di distribusikan kepada client. untuk melakukan konfigurasi dapat dilakukan dengan perintah:

   ```
   # sudo ./openvpn-install.sh.
   ```

   Setelah semua proses penginstallan dan konfigurasi pada OpenVPN server dilakukan maka hasil yang didapatkan adalah sudah terdapatnya ip tun atau tunnel sorftware network interface pada interface configuration di server. Konfigurasi server OpenVPN dapat dilihat pada file /etc/openvpn/server/ server.conf, pengaturan atau konfigurasi yang dapat dilihat dan di ubah pada file server.conf tersebut adalah OpenVPN server ip, DNS, port, dan porto. Tujuan penginstalan OpenVPN adalah untuk membuat sebuah client baru, dalam bentuk sebuah file berekstensi .ovpn yang berisi konfigurasi untuk dapat connect ke server, dan file tersebut akan dibagikan kepada client nantinya agar dapat koneksi ke jaringan OpenVPN dari server. OpenVPN merupakan aplikasi open-source untuk membuat Virtual Private Network (VPN) aplikasi yang dapat terkoneksi point-to-point tunnel yang telah terenkripsi. Setelah Install OpenVPN, agar config OpenVPN yang dibuat dapat dipakai oleh client, dapat dilakukan dengan cara transfer config tersebut melalui koneksi SFTP dengan aplikasi FilleZila.

*3.3. Koneksi OpenVPN Client*

Tujuan dari penginstallan OpenVPN client adalah agar client dapat melakukan koneksi ke jaringan VPN yang diberikan server, agar bisa melakukan koneksi, client harus membuka aplikasi OpenVPN client terlebih dahulu, lalu import file config OpenVPN dan lakukan koneksi, hasil dari koneksi OpenVPN. Tujuan dari menjalankan service API pada jaringan OpenVPN adalah untuk melakukan testing antar client. Langkah pertama yang dilakukan connect OpenVPN di PC, lalu buatlah sebuah API, Setelah membuat sebuah API, jalankan API tersebut pada ip yang di dapat dari OpenVPN, Setelah melakukan setting pada route API, selanjutnya running dengan menggunakan local camel context

*3.4. Pengujian*

Setelah melakukan proses implementasi, langkah selanjutnya yaitu melakukan proses pengujian sistem yang telah dibuat. Proses ini bertujuan untuk melihat apakah sistem menghasilkan hasil yang diinginkan dan sesuai dengan fungsi dari sistem tersebut. Proses pengujian di lakukan pada postman untuk memastikan bahwa rancangan yang dibuat memiliki keluaran yang sesuai dengan yang diharapkan.

**TABEL 1.** Data Hasil PEngujian

| No | Uji Fungsi | Detai Pengujian | Hasil Pengujian |
|---|---|---|---|
| 1 | AWS server | Running | Berhasil |
| 2 | OpenVPN Server | Running | Berhasil |
| 3 | OpenVPN Client | Running | Berhasil |
| 4 | Private Spring API pada Server | Running | Berhasil |
| 5 | Private Spring API pada client-10.8.0.2 | Running | Berhasil |
| 6 | Remote Server dengan FileZilla menggunakan jaringan OpenVPN | Running | Berhasil |
| 7 | Request pada API yang terinstall pada client- 10.8.0.2 menggunakan aplikasi mobile pada client-10.8.0.3 | Running | Berhasil |
| 8 | Request pada API yang terinstall pada client-10.8.0.2 menggunakan postman pada client-10.8.0.4 | Running | Berhasil |

engujian pada perubahan ip address client bertujuan untuk mengetahui perubahan yang terjadi saat client tidak terkoneksi dengan OpenVPN, dan dibandingkan dengan saat terkoneksi dengan OpenVPN. Dari pengujian ini dapat ditarik kesimpulan, ketika client tidak terkoneksi pada jaringan OpenVPN maka client hanya memiliki ip yang di dapat dari wifi

Pengujian Kecepatan jaringan ini akan dilakukan dengan cara membandingkan kecepatan jaringan client saat sebelum melakukan koneksi pada jaringan OpenVPN, dan setelah koneksi pada jaringan OpenVPN.

Pengujian Koneksi bertujuan untuk mlakukan uji coba terhadap jaringan OpenVPN yang telah di berikan oleh host dan dijalankan pada perangkat client. Pengujian dilakukan dengan menggunakan aplikasi FileZilla untuk melakuka remote server dari computer client. Langkah pertama adalah membuka FileZilla, lalu kemudian memasukkan gateway OpenVPN, atau ip OpenVPN server, dengan port yang digunakan 22.

Pengujian pada postman dilakukan dengan tujuan untuk melakukan uji coba apakah API berjalan dengan baik. Masukkan hosname atau url API yang sudah di deploy sebelumnya ke kolom url, lalu tentukan method yang dipakai oleh API (Post/Get), lalu lakukan send request.

## 4. KESIMPULAN

Setelah Implementasi serta pengujian terhadap perancangan openvpn server menggunakan ubuntu server 20.04 lts dapat diambil beberapa kesimpulan sebagai berikut: Pembuatan OpenVPN Server sebagai tunnel untuk menghubungkan antar client dengan client, maupun client dan server berhasil di buat. Implementasi OpenVPN server untuk Java REST API yang berjalan pada komputer client yang di request oleh client android berhasil dilakukan. Kecepatan koneksi bergantung pada besarnya kecepatan upstream koneksi internet pada OpenVPN Server. Sistem ini dapat dimanfaatkan untuk keperluan remote antar perangkat yang terhubung dengan jaringan OpenVPN.

## REFERENSI

[1] Sunyoto, Wendy, Aris, VPN Sebuah Konsep Teori dan Implementasi, Buku Web Networking, Surabaya, 2006.

[2] Sunyoto, Wendy, Aris,, Ramadhana ,SS,Ahmad, Membangun VPN Linux Secara Cepat, Andi, Jakarta, 2005.

[3] N. Karimi. (2013, Novermber 19). “How To Setup a Multi-Protokol VPN Server Using SoftEther” [online]. Available: https://www.digitalocean.com/community/tutorials/how-to-setup-a-multi-Protokol-vpn-Server-usingsoftether.

[4] Pribadi. T.P. 2013. Implementasi High-Availability VPN Client Pada Jaringan Komputer Fakultas Hukum Universitas Udayana. Bandung: Jurnal Ilmu Komputer. Vol. 6, No.1:21.

[5] Susanto.T.R., Indriyanta. G., dan Santosa. G.R. Analisis Perbandingan Performa Point To Point Tunneling Protocol Dan Ethernet Over Internet Protocol Dalam Membentuk VPN.Yogyakarta: Jurnal Informatika. Vol. 9, No.1:12-15.

[6] Sofana, Iwan. 2013. Membangun Jaringan Komputer. Bandung : Informatika.

[7] Syafrizal, Melwin. 2008. Pengantar Jariangan Komputer. Yogyakarta : Andi.

[8] Sunyoto, Wendy, Aris, VPN Sebuah Konsep Teori dan Implementasi, Buku Web Networking, Surabaya, 2006.

[9] Sunyoto, Wendy, Aris,, Ramadhana ,SS,Ahmad, Membangun VPN Linux Secara Cepat, Andi, Jakarta, 2005.

[10] N. Karimi. (2013, Novermber 19). "How To Setup a Multi-Protokol VPN Server Using SoftEther" [online]. Available : https://www.digitalocean.com/community/tutorials/how-to-setup-a-multi- Protokol-vpn-Server-usingsoftether.

[11] S. Wardoyo, T. Ryadi, and R. Fahrizal, "Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni dan Tunneling 6to4 Berbasis Router Mikrotik," J. Nas. Tek. Elektro, vol. 3, no. 2, p. 106.

[12] Pribadi. T.P. 2013. Implementasi High-Availability VPN Client Pada Jaringan Komputer Fakultas Hukum Universitas Udayana.Bandung: Jurnal Ilmu Komputer. Vol. 6, No.1:21.

[13] Susanto.T.R., Indriyanta. G., dan Santosa. G.R. Analisis Perbandingan Performa Point To Point Tunneling Protocol Dan Ethernet Over Internet Protocol Dalam Membentuk VPN.Yogyakarta: Jurnal Informatika. Vol. 9, No.1:12-15.

[14] Sofana, Iwan. 2013. Membangun Jaringan Komputer. Bandung : Informatika.

[15] Syafrizal, Melwin. 2008. Pengantar Jariangan Komputer. Yogyakarta : Andi.

[16] Astawa dkk. Implementasi Vpn Pada Jaringan Komputer Kampus Puliteknik Negri Bali. 2012 Bali.

[17] Hendra. 2006. Belajar Sendiri Cisco ADSL Router, PIX Firewall, dan VPN. Jakarta: PT. Elex Media Komputindo

[18] Madcom. 2010. Sistem Jaringan Komputer untuk Pemula. Madiun: Andi

[19] Markus F. 2006. OpenVPN, Building and Integrating Virtual Private Networks.Birmingham: Packt Publishing Ltd

[20] Melwin S. 2005. Pengantar Jaringan Komputer. Yogyakarta: Andi Offset

[21] Paulus YJ. 2012, Computer Networking, Pengaturan Jaringan, Keamanan Jaringan, Koneksi dan sharing, Troubleshooting Jaringan. Yogyakarta: Andi

[22] Winarto E, Zaki A, & Community. 2013. Membuat Sendiri Jaringan Komputer.Semarang: PT. Elex Media Komputindo.

[23] Prihatin Oktivasari & Andri Budhi Utomo, Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol

[24] Prasetyo U. Rompas, Arie S.M. Lumenta, Arthur M. Rumagit, Brave A. Sugiarso, Implementasi Openvpn Server Untuk Koneksi Remote Pada Perangkat Android, Vol 1, No 3 (2012).

[25] Mohammad Badrul, Open VPN-Access Server Dengan Enskripsi SSL/TI Open SSL, Vol.1, No. 1, Desember 2016, 1 - 12.