

## RANCANG BANGUN PANEL VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WEB

Mukhammad Rizki Novanto, Joseph Dedy Irawan, F. X Ariwibisono

Program Studi Teknik Informatika S1, Fakultas Teknologi Industri  
Institut Teknologi Nasional Malang, Jalan Raya Karanglo km 2 Malang, Indonesia  
rizkinovanto@hotmail.com

### ABSTRAK

Semenjak pandemi virus Covid-19 kegiatan internet terus menjadi bertambah. Semacam halnya bekerja dari rumah memakai internet, belajar daring memakai internet, komunikasi social media memakai internet, belanja online di pasar online dengan internet, sampai mencari data lewat internet. Kebutuhan internet terus menjadi bertambah, tidak hanya harga virtual private server yang disediakan provider lokal relatif mahal serta instalasi sampai operasional membutuhkan banyak tahapan, semacam wajib menginstal script guna berjalannya protocol pada VPS sehingga dibutuhkannya sesuatu system website yang bisa jadi fasilitas buat mengakses sampai membuat akun *virtual private network*. Bermacam tipe VPN yang terletak pada VPS bisa dikelola via website oleh admin. *User* bisa melaksanakan pembuatan akun VPN pada website. Pada biasanya bila mau mengakses VPN wajib login VPS terlebih dulu buat membuat VPN. Berbentuk username & passwordsampai expired dan perinci pelayanan sampai port yang hendak digunakan pada *protocol* VPN semacam SSH, V2RAY, Trojan, L2TP, Shadowsocks. Perihal ini dirasa kurang efektif semacam login *terminal* VPS dulu buat membuat akun VPN secara manual, buat memudahkan client diperlukan panel berbasis website. Diharapkan bisa memudahkan pengguna dalam membuat VPN via website serta tidak wajib login VPS terlebih dulu. Menyederhanakan perintah dari VPS yang diimpelentasikan via website hendak memudahkan kegiatan user dalam pembuatan VPN. Berdasarkan hasil akhir, Web GUI yang telah menyediakan fitur layanan VPN sesuai yang disediakan VPS berjalan dengan normal. Masing-masing protokol atau jenis VPN memiliki karakteristik daya kinerja yang berbeda. Meliputi kecepatan dan *ping* pada saat diuji coba melalui alamat website *speedtest.net* untuk mengukur kecepatan dan *ping* koneksi internet.

**Kata kunci :** VPN, VPS, V2RAY, L2TP, Shadowsocks, Trojan, SSH

### 1. PENDAHULUAN

Tidak dapat dipungkiri sejak pandemi virus Covid-19 aktivitas internet semakin meningkat. Seperti halnya bekerja dari rumah menggunakan internet, belajar daring menggunakan internet, komunikasi social media menggunakan internet, belanja online di marketplace dengan internet, hingga mencari informasi melalui internet.

Kebutuhan internet semakin meningkat, selain harga virtual private server yang disediakan provider lokal relatif mahal dan instalasi hingga operasional memerlukan banyak tahapan, seperti harus menginstal script untuk fungsi berjalannya protocol pada VPS sehingga dibutuhkannya suatu system web yang dapat menjadi sarana untuk mengakses hingga membuat akun virtual private network . Berbagai macam jenis VPN yang berada pada VPS dapat dikelola via web oleh admin. User dapat melakukan pembuatan akun VPN pada web.

Diharapkan dapat mempermudah pengguna dalam membuat VPN via web dan tidak harus login VPS terlebih dahulu. Menyederhanakan perintah dari VPS yang diimpelentasikan via web akan mempermudah aktivitas user dalam pembuatan VPN Pada umumnya jika ingin mengakses VPN harus login VPS terlebih dahulu untuk membuat VPN. Berupa username & password hingga expired serta detail pelayanan hingga port yang akan digunakan pada protocol VPN seperti SSH, V2ray, Trojan, L2tp,

Shadowsocks. Hal ini dirasa kurang efisien seperti login terminal VPS dahulu untuk membuat akun VPN secara manual, untuk mempermudah client dibutuhkan panel berbasis web.

### 2. TINJAUAN PUSTAKA

#### 2.1. Penelitian Terkait

Pada umumnya VPS menyediakan layanan beberapa jenis VPN. Ketika ada kebutuhan ingin mengakses VPN, maka harus login ke VPS dahulu untuk memberikan hak akses. Jikalau sudah terkoordinasi dengan panel web VPN. Semua layanan akan dapat dipermudah pengguna dalam mengaksesnya.

#### 2.2. VPN

VPN (Virtual Private Network) merupakan suatu cara untuk membuat jaringan bersifat private dan aman dengan menggunakan jaringan publik, misalnya internet. VPN (Virtual Private Network) adalah variasi jaringan komputer yang tingkatannya lebih advanced dibandingkan jaringan komputer biasa. Data-management subsystem, meliputi basis data yang berkaitan dengan permasalahan terkait, mengontrol seluruh jaringan computer lalu lintas ke Internet melewati VPN, tetapi sebagian besar bersifat domestik. Orang yang menggunakan VPN, menggunakan beberapa vendor VPS. [7]



Gambar 1. Ilustrasi VPN

### 2.3. VPS

Virtual Private Server (VPS) merupakan suatu jenis server yang memakai teknologi virtualisasi buat membagi hardware server raga jadi sebagian server virtual yang di hosting di infrastruktur raga yang sama. Di jaman dulu, sistem *administrator* secara tradisional cuma mempunyai satu server raga serta cuma digunakan buat satu tujuan saja. Sedangkan virtualisasi menawarkan kemudahan buat melakukan *host* sebagian server pada satu server raga. Tiap server bisa mempunyai tujuan mereka sendiri serta sistem pembedahan yang berbeda satu sama lain. Perihal ini bisa menolong mengimprovisasi tingkatan fleksibilitas yang ada pada administrator sistem dalam perihal pemilihan konfigurasi aplikasi yang bisa mereka jalankan. Tidak hanya itu, ini pula bisa membagikan keuntungan yang signifikan dalam perihal skalabilitas dari energi pemrosesan (processing power), RAM, serta disk ruang dengan bayaran yang lebih rendah daripada memakai hardware raga tradisional. VPS pula bisa difungsikan selaku server VPN.[8]



Gambar 2. Ilustrasi VPS

### 2.4. Trojan

Trojan menggunakan teknologi komunikasi terowongan HTTP, makalah ini mempelajari untuk mendeteksi kuda Trojan terowongan HTTP berbasis. Ujung kendali program kuda Trojan membuka jalan ke monitor 80 port, tidak membuat server Web nyata untuk menanggapi permintaan HTTP, itu hanya menerima informasi yang dikirim oleh terminal yang dikendalikan.[14]



Gambar 3. Ilustrasi Trojan

### 2.5. L2TP

L2TP merupakan tunneling yang bekerja di layer 2, namun L2TP tidak mempunyai pengamanan

spesial sehingga umumnya ditambahkan sistem keamanan yang lebih baik, ialah memakai IPSec. Pengamanan VPN dengan memakai enkripsi tertentu sangat dibutuhkan supaya informasi yang melewati tunneling untuk dikemudian nantinya akan dapat dilindungi kerahasiannya.[5]



Gambar 4. Ilustrasi L2TP

### 2.6. SSH

SSH ialah protokol jaringan yang membolehkan buat melaksanakan komunikasi pertukaran informasi lewat saluran nyaman antara 2 device jaringan. SSH tidak hanya itu SSH pula menunjang fitur buat pengiriman berkas ataupun file lewat SFTP (secure File Transfer Protocol) ataupun SCP (Secure Copy). SSH memakai model komunikasi client-server. Standart port dari ssh merupakan port 22 yang sudah diresmikan selaku jalan buat server SSH. Suatu klien SSH umumnya digunakan buat membangun koneksi antara klient dengan server SSH biar bisa dikendalikan via kendali jarak jauh.[9]



Gambar 5. Ilustrasi SSH

### 2.7. V2RAY

V2Ray lebih baik dari Shadowsocks Protokol, kinerja yang lebih kuat, dan fitur yang lebih dari Shadowsocks. V2Ray memiliki fleksibilitas untuk meneruskan, langsung menghubungkan, atau memblokir bagian Sub-koneksi, fleksibel melalui kombinasi yang berbeda dari protokol masuk dan keluar. Mengkonversi format komunikasi. Ambil teknologi multipleks untuk lebih meningkatkan kinerja bersamaan dari Internet, dan perubahan dinamis dari komunikasi, Untuk menghindari pembatasan kecepatan pemblokiran pada port lalu lintas tinggi. Tentu saja, V2Ray baru saja rilis, dan rantai industri belum selesai. Proses konfigurasi lebih rumit daripada Shadowsocks.[7]



Gambar 6. Ilustrasi V2RAY

## 2.8. Shadowsocks

Dalam beberapa tahun terakhir, metode proxy berbasis Socks5 telah disebut Protokol transmisi enkripsi Shadowsocks dimulai Shadowsocks menolak ketika menembus firewall sehingga sangat mengganggu dan membingungkan mengenkripsi lalu lintas. Dalam penggunaan Shadowsocks ketika semua lalu lintas sama melalui firewall. Pada dasarnya diakui sebagai lalu lintas normal, lebih stabil daripada VPN dan harga yang lebih rendah.[8]



Gambar 7. Ilustrasi Shadowsocks

## 2.9. PHP

PHP (Hypertext Preprocessor) merupakan bahasa pemrograman *open source* yang digunakan buat membuat suatu aplikasi website. PHP Hypertext Preprocessor ialah pemrograman server side, ialah bahasa yang berjalan di sisi server. Kode program PHP hendak dieksekusi oleh server serta hasil eksekusi tersebut hendak disuguhkan kepada client [11]



Gambar 8. Ilustrasi PHP

## 2.10. XAMPP

Xampp ialah singkatan dari X (4 sistem pembedaan apapun), XAMPP ialah fitur lunak leluasa, yang menunjang banyak sistem pembedaan, serta ialah kompilasi dari sebagian program. Semacam Apache, MYSQL, PHP, serta Perl. Xampp merupakan alat yang sediakan paket fitur lunak dalam satu buah paket. Dalam paket Xampp telah ada Apache (*Website Server*), Mysql (*Database*), PHP (*server side scripting*), Perl, FTP server, PhpMyAdmin.[12]



Gambar 9. Ilustrasi XAMPP

## 2.11. HTML

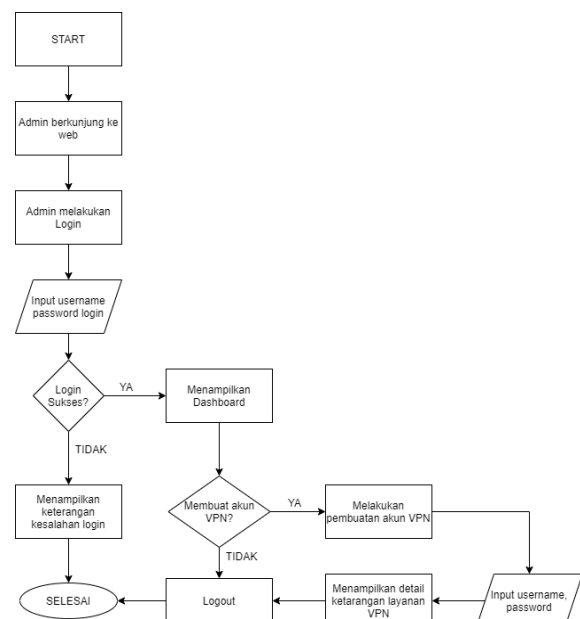
Hypertext Markup Language( HTML) merupakan bahasa standard yang digunakan buat menunjukkan taman website". Yang dapat dicoba dengan HTML ialah; Mengendalikan tampilan dari taman website serta isinya, membuat tabel dalam taman website, mempublikasikan laman website secara online, membuat form yang dapat digunakan buat menanggulangi pendaftaran serta transaksi via website. Contoh: Tiap dokumen HTML dimulai serta diakhiri dengan tag HTML [13]



Gambar 10. Ilustrasi HTML

## 3. DESAIN DAN PERANCANGAN

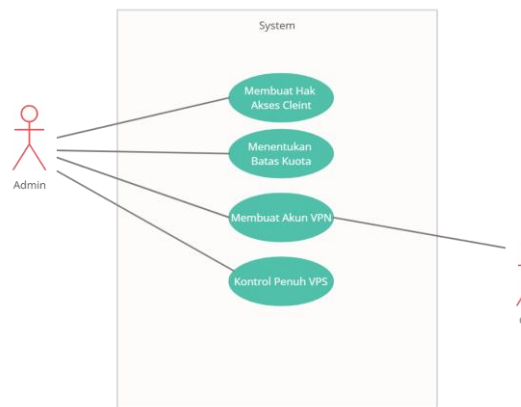
### 3.1. Flowchart Sistem



Gambar 11. Tampilan flowchart sistem

Pada diagram alur diatas menjelaskan bagaimana urutan penggunaan system. Admin akan melakukan login dengan meinputkan username serta password login yang valid dan benar. Jikalau login sudah sukses akan menampilkan tampilan dari dashboard, jika salah akan menampilkan keterangan kesalahan login. Pada menu dashboard akan disediakan menu pembuatan akun beberapa jenis VPN. Jikalau ingin melakukan pembuatan akun VPN, akan meinputkan username dan password yang diinginkan, jikalau tidak akan log out dan selesai. Setelah meinputkan username dan password yang akan digunakan pada layanan VPN, akan ditampilkan detail keterangan dari layanan VPN tersebut.

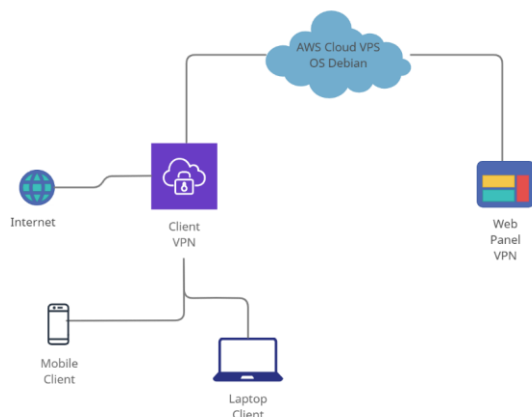
### 3.2. Use Case



Gambar 12. Use Case

Pada Gambar 12 merupakan hubungan interaksi admin dengan system yaitu admin berperan dalam membuat hak akses client, menentukan batas kuota, membuat akun VPN, dan control penuh VPS. Client hanya dapat membuat akun VPN. Kendali keteknisan fitur dipegang penuh oleh admin. Sehingga ada batasan untuk client dalam menggunakan panel web tersebut.

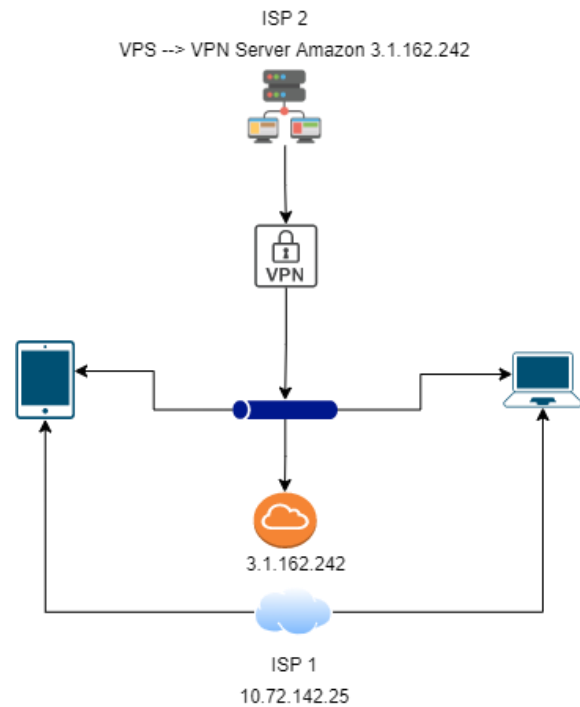
### 3.3. Rancangan Blok Diagram Sistem



Gambar 13. Tampilan desain system

Pada gambar 13 Rancangan Blok Diagram Sistem AWS Cloud VPS yang sudah terinstal *protocol* VPN, akan terhubung dengan website. User dapat melakukan pembuatan akun VPN via website. Client yang telah terhubung dengan internet dapat menggunakan akun VPN hingga bisa terkoneksi dengan VPN dengan IP 3.1.142.262. Layanan *protocol* VPN yang ada pada VPS telah ditransformasikan dengan menu Web GUI Panel VPN.

### 3.2 Topologi Sistem

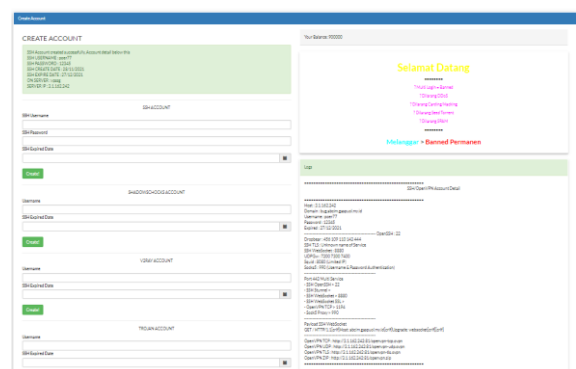


Gambar 14. Topologi Sistem

Topologi VPN Server Amazon dengan IP 3.1.162.242 dalam keadaan terinstal *protocol* VPN lalu layanannya ada pada Web GUI Panel VPN. Perangkat client berupa gadget handphone dan laptop terhubung ke internet dengan layanan ISP 1 dengan IP (misal) 10.72.142.25 dapat melakukan akses VPN dengan menggunakan fitur default gadget atau aplikasi yang menyediakan fitur untuk menjalankan VPN seperti contohnya netmod for pc, atau v2rayNG untuk HP. Setelah client menjalankan aplikasi VPN dengan akun VPN dengan IP 3.1.162.242. Otomatis IP dari ISP 1 10.72.142.25 akan berubah menjadi IP VPN 3.1.162.242.

## 4. HASIL DAN PEMBAHASAN

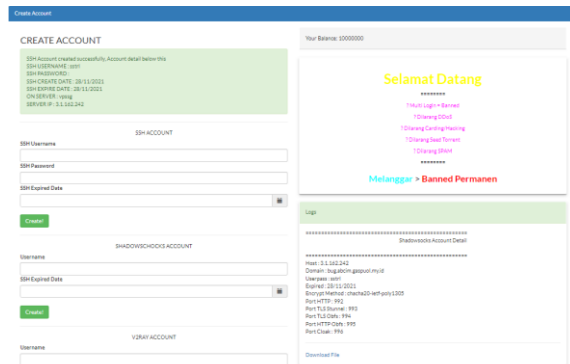
### 4.1. Tampilan Create SSH Success



Gambar 14. Tampilan Create SSH Success

Terdapat informasi berhasilnya pembuatan akun SSH dengan username dan password yang telah diinputkan lalu pada log tertera detail layanan yang bisa digunakan client. Muncul banner selamat datang berwarna berisi notice..

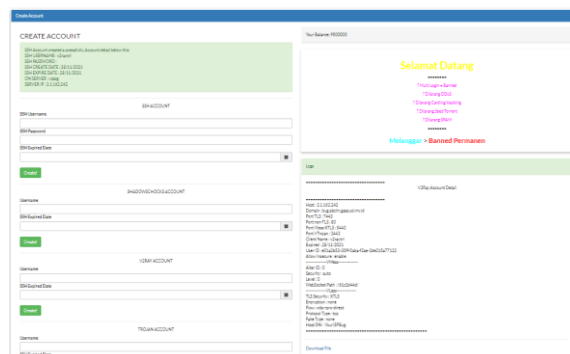
#### 4.2. Tampilan Create Shadowsocks Success



Gambar 15. Tampilan Create Shadowsocks

Terdapat informasi berhasilnya pembuatan akun Shadowsocks dengan username dan password yang telah diinputkan lalu pada log tertera detail layanan yang bisa digunakan client. Muncul banner selamat datang berwarna berisi notice.

#### 4.3. Tampilan Create V2RAY Success

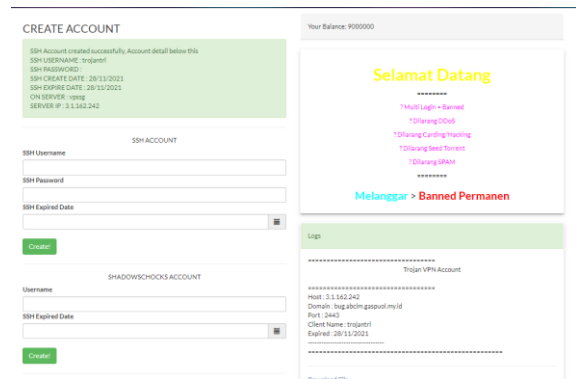


Gambar 16. Tampilan Create V2RAY Success

Pada gambar 16 di Halaman Create V2RAY Success terdapat informasi berhasilnya pembuatan akun V2RAY dengan username dan password yang telah diinputkan lalu pada log tertera detail layanan yang bisa digunakan client. Muncul banner selamat datang berwarna berisi notice.

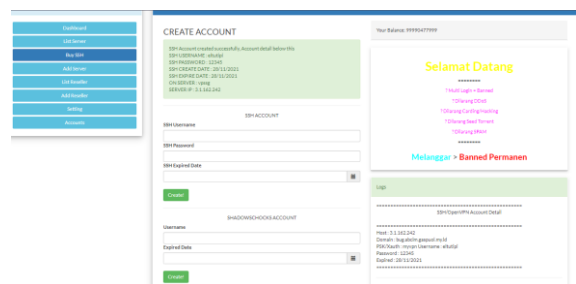
#### 4.4. Tampilan Create Trojan Success

Terdapat informasi berhasilnya pembuatan akun Trojan dengan username dan password yang telah diinputkan lalu pada log tertera detail layanan yang bisa digunakan client. Muncul banner selamat datang berwarna berisi notice.



Gambar 17. Tampilan Create Trojan Success

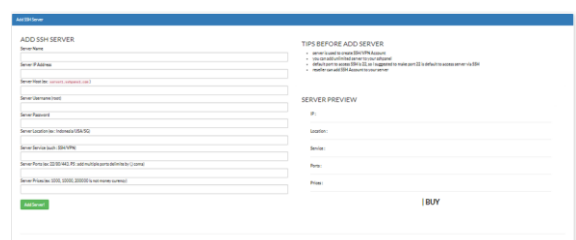
#### 4.5. Tampilan Create L2TP Success



Gambar 18. Tampilan Create L2TP Success

Terdapat informasi berhasilnya pembuatan akun Trojan dengan username dan password yang telah diinputkan lalu pada log tertera detail layanan yang bisa digunakan client. Muncul banner selamat datang berwarna berisi notice.

#### 4.6. Tampilan Halaman Add Server



Gambar 19. Tampilan halaman Add Server

Pada Gambar 19. merupakan tampilan halaman Add Server terdapat informasi untuk menambah server yaitu Server Name merupakan nama server, Server IP Address merupakan alamat IP numerik server, Server Host merupakan domain host server, Server username (root), Server password, Server Location, Server Service, Port server dan Server prices harga per create VPN

#### 4.7. Tampilan Halaman Edit Server

Gambar 20. Tampilan Halaman Edit Server

Terdapat informasi untuk edit server yaitu Server Name merupakan nama server, Server IP Address merupakan alamat IP numerik server, Server Host merupakan domain host server, Server username (root), Server password, Server Location, Server Service, Port server dan Server prices harga per create VPN.

#### 4.8. Tampilan Halaman List Server

Server Name	IP	Host	Location	Action
vpssg	3.1.162.242	bug.abcim.gaspool.my.id	SG	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Reboot</a>

Gambar 21. Tampilan Halaman Hasil

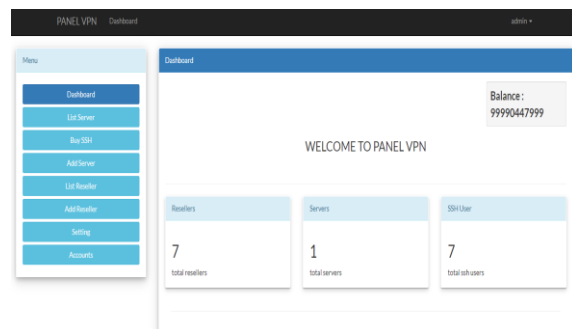
Pada gambar 21 di halaman List Server terdapat informasi Server Name merupakan nama server yaitu vpssg, dengan IP 3.1.162.242, host domain bug.abcim.gaspool.my.id, Lokasi Singapura (SG). Action aksi Edit server, Delete server, Reboot Server dan List User.

#### 4.9. Tampilan Halaman Create Account

Gambar 22. Tampilan Halaman Create Account

Pada gambar 22 di halaman Create Account terdapat informasi jenis atau protocol VPN yang dapat dibuat yaitu SSH, Shadowsocks, V2RAY, Trojan, dan L2TP. Menginputkan username dan password serta masa expired lalu create.

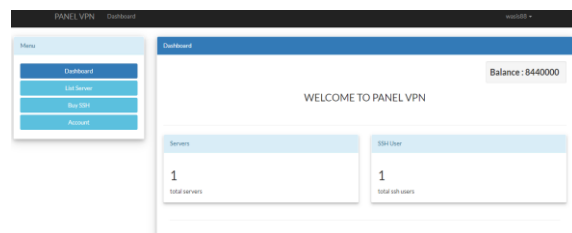
#### 4.10. Tampilan Dashboard Admin



Gambar 23. Tampilan Halaman Create Account

Terdapat beberapa informasi yaitu Resellers, Servers, dan SSH User. Untuk halaman administrator menu yang dapat diakses adalah menu List Server, Buy SSH, Add Server, List Reseller, Add Reseller, Setting, dan Accounts.

#### 4.11. Tampilan Dashboard Resellers



Gambar 24. Tampilan Halaman Create Account

Terdapat informasi servers dan ssh user, dan hanya terdapat menu dashboard list server, buy ssh, dan account.

#### 4.12. Pengujian Fungsional Sistem

Pengujian fungsional sistem dilakukan untuk menguji fitur-fitur yang ada pada aplikasi. Hasil pengujian fungsional sistem ditunjukkan dalam Tabel berikut. Menggunakan Browser Mozilla Firefox dan Google Chrome



Tabel 1. Pengujian Sistem

No	Fungsi Yang Diuji	Mozilla Firefox	Google Chrome
1	Login	√	√
2	Halaman List Server	√	√
	a. Edit Server	√	√
	b. Delete Server	√	√
	c. Reboot Server	√	√
3	Halaman Data Create Server	√	√
	a. Create Ssh Account	√	√
	b. Create Shadowsocks Account	√	√
	c. Create V2ray Account	√	√
	d. Create Trojan Account	√	√
	e. Create L2tp Account	√	√
4	Halaman Add Server	√	√
	a. Add Server	√	√
5	Halaman List Reseller	√	√
	a. Edit Data Reseller	√	√
	b. Delete Data Reseller	√	√
	c. Topup Balance Reseller	√	√
6	Halaman Add Reseller	√	√
7	Halaman Setting	√	√
	a. Set SSH Price	√	√
	b. SSH User	√	√
7	Halaman Account	√	√
	a. Change Email	√	√
	b. Change Username	√	√
	c. Change Password	√	√
10	List SSH Account	√	√
	a. Delete Account	√	√
11	Logout	√	√

Keterangan :

√ = Berhasil

X = Gagal

Berdasarkan hasil pengujian fungsional sistem yang telah dilakukan mendapatkan hasil bahwa pada aplikasi Panel VPN, fungsional yang dibuat telah berhasil dan berjalan dengan baik.

#### 4.13. Pengujian VPN

Pengujian VPN dilakukan untuk menguji status berjalan atau tidak di perangkat client, pada masing-masing jenis atau protocol VPN. Hasil pengujian VPN ditunjukkan dalam Tabel berikut. Menggunakan Perangkat Handphone dan Laptop

Tabel 2. Pengujian VPN

No	Fungsi Yang Diuji	Handphone	Laptop	Ket. Aplikasi VPN HP	Ket. Aplikasi VPN Laptop
1	SSH Account	√	√	Http Injector Lite	Netmod
2	Shadowsocks Account	√	√	V2rayNG	Shadowsocks for PC
3	V2ray Account	√	√	V2rayNG	Netmod
4	Trojan Account	√	X	V2rayNG	-
5	L2TP Account	√	X	VPN L2TP HP	VPN L2TP Windows 10

Keterangan :

√ = Berhasil

X = Gagal

Berdasarkan hasil pengujian VPN yang telah dilakukan mendapatkan hasil bahwa pada aplikasi VPN, fungsional yang dibuat telah berhasil dan berjalan dengan baik pada perangkat HP, sedangkan pada perangkat laptop gagal pada Trojan dan L2TP.

#### 4.14. Pengujian Kecepatan VPN

Pengujian performa VPN dilakukan untuk menguji performa kecepatan pada masing-masing jenis atau protocol VPN. Hasil pengujian VPN ditunjukkan dalam Tabel berikut. Menggunakan Perangkat Handphone dan Laptop pada speedtest.net

Tabel 3. Pengujian Performa VPN

No	VPN Yang Diuji	Speedtest-1 DL/UL	Speedtest-2 DL/UL	Speedtest-3 DL/UL	Speedtest-4 DL/UL	Speedtest-5 DL/UL
1	SSH Account	9,99/1,76	10,1/4,18	19,7/3	12,1/3,71	12,6/8,54
2	Shadowsocks Account	18,6/9,75	20,5/2,76	7,66/5,27	8,80/3,68	15,8/4,82
3	V2RAY Account	7,89/4,78	14,7/3,40	12,8/1,07	7,53/11,6	3,68/6,37
4	Trojan Account	12,7/2,60	21,1/5,62	5,02/15,7	14,7/5,16	13,6/11,3
5	L2TP Account	10,3/3,81	13/2,61	14,8/2,64	4,75/4,81	15,9/3,79

Keterangan :

√ = Berhasil

X = Gagal

DL/UL : Download/Upload

ms : millisecond

Berdasarkan hasil pengujian kecepatan VPN yang telah dilakukan, bahwasannya setiap percobaan beberapa kali dari masing-masing protocol VPN mendapatkan hasil yang berbeda-beda. Mengikuti keadaan sumber koneksi internet utama.49,21 Mbps serta 21,5 kecepatan upload.

## 5. KESIMPULAN

Kesimpulan yang bisa dijabarkan dari hasil pembuatan aplikasi panel virtual private network berbasis website. Aplikasi panel virtual private network berbasis website ini sukses membagikan layanan VPN. Bersumber pada hasil pengujian fungsionalitas pada aplikasi ini bisa dijalankan dengan baik pada browser website, Bersumber pada hasil pengujian system, tidak terdapatnya fitur yang tidak berjalan menunjukkan sistem berjalan 100%. Bersumber pada hasil pengujian aplikasi dengan memakai 2 browser yang berbeda, seluruh tampilan serta guna aplikasi bisa berjalan 100% pada 2 browser ialah, Mozilla Firefox serta Google Chrome.

## DAFTAR PUSTAKA

- [1] Prianto, I. A., & Muhammad Kusban, S. T. (2016). *Simulasi Dan Perbandingan PSAD, Suricata Untuk Mencegah Scanning Port Oleh Zenmap Pada VPS Ubuntu* (Doctoral dissertation, Universitas Muhammadiyah Surakarta).
- [2] Habibi, A., & Arifin, S. (2015). Membangun Jaringan Virtual Private Network (VPN) dengan Metode Tunneling Menggunakan Mikrotik untuk Komunikasi Lokal Di Stmik Ppkia Pradnya Paramita Malang. *Jurnal Teknologi Informasi: Teori, Konsep, dan Implementasi*, 6(2), 115-119.
- [3] Supriyanto, B., & Suharyanto, S. (2019). Perancangan Jaringan VPN Menggunakan Metode Point to Point Tunneling Protocol. *Jurnal Teknik Komputer*, 5(2), 235-240.
- [4] Pratama, R., Orisa, M., & Ariwibisono, F. X. (2020). APLIKASI MONITORING DAN CONTROLLING SERVER MENGGUNAKAN PROTOCOL ICMP (INTERNET CONTROL MESSAGE PROTOCOL) DAN SSH (SECURE

- SHELL) BERBASIS WEBSITE. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 4(1), 397-403.
- [5] Roseno, Muhammad Taufik, "Analisis Perbandingan Protokol Virtual Private Network (VPN) - PPTP, L2TP, IPSEC - Sebagai Dasar Perancangan VPN pada Politeknik Negeri Sriwijaya". 2013.
- [6] Lukman Sahni, Lukman, "Perancangan, Implementasi, dan Analisa Perbandingan L2TP/IPSec VPN dengan OpenVPN pada Mikrotik Router", Bandung: Institute Teknologi Telkom, 2012.
- [7] G, Rajeev. G, Samta Jain, "A Review On Layer 2 Tunneling Protocol", *International Journal of Application or Innovation in Engineering & Managemen*, Volume 3, Issue 10, 2014, pp 307-310.
- [8] Zhang Zhengxu, and Xu Yuan. "Analysis and Research on Internet Proxy Plug-ins under Network Supervision." *Cyberspace Security* 11.6 (2020): 9.
- [9] Shuye, et al. "A method for detecting and identifying VPN encrypted traffic based on segmented entropy distribution." *Cyberspace Security* 11.8 (2020): 5
- [10] Luo Youqiang, et al. "DNS tunnel Trojan detection method based on communication behavior analysis." *Journal of Zhejiang University (Engineering Science Edition)* 51.9 (2017): 1780-1787.
- [11] Andi Yogyakarta, Wahana Komputer/Sistem Informasi Penjualan Online, Yogyakarta
- [12] Anak Puspita Rahastri, Tengku A. Riza, ST., Rohmat Tulloh. 2015. Perancangan dan Implementasi Sistem Informasi Sekolah (Studi Kasus Smp N 2 Patikraja Banyumaas *Jurnal E-Procedding of Apllied Science*. Vol. 1. No. 3, Hal. 2660-2666, ISSN: 2442-5826
- [13] Fitri Ayu, N. P. (2018). 2) 1,2. Perancangan Sistem Informasi Pengolahan Data Praktek Kerja Lapangan (PKL), 2(2), 12–26.
- [14] Wu, Ting. "Research on adaptive network theft Trojan detection model." (2015).