JACKA
Journal of Advanced Computer Knowledge and Algorithms
Vol. 1, No. 3, July, 2024, pp. 79-83
Journal homepage: http://ojs.unimal.ac.id/jacka

Virtual Private Cloud (VPC) & Elastic Compute Cloud (EC2) with Remote Access Using PuTTY Terminal on Ubuntu in a Private VPN

Irwanda Syahputra[1*], Rizalul Akram[2]

[1] Universitas Sains Cut Nyak Dhien, Indonesia
[2] Universitas Samudra, Indonesia

[*]Corresponding Author Email: irwanda.syahputra@gmail.com

Received: 26 June 2024
Revised: 30 June 2024
Accepted: 1 July 2024
Available online: 1 July 2024

Kata Kunci:
VPN, VPC, EC2, PuTTY Gen Terminal Ubuntu

ABSTRAK

Salah satu teknologi komputer yang umum digunakan oleh instansi/perusahaan adalah jaringan internet yang berfungsi sebagai jembatan penghubung antara satu titik dengan titik yang lain. Selain memiliki manfaat sebagai salah satu media dalam berkomunikasi jarak jauh, internet juga memiliki kekurangan dari tingkat keamanannya. Salah satu kendala yang dihadapi yaitu internet sebagai media transmisi data-data yang bersifat penting atau confidential. Salah satu upaya yang dapat dilakukan untuk mengatasi permasalahan tersebut adalah dengan membangun sebuah jaringan privasi dalam sebuah layanan jaringan publik, atau yang sering dikenal dengan Virtual Private Network (VPN). Pada penelitian ini VPN dibangun dengan mengkombinasikan Virtual Private Cloud (VPC) dengan Elastic Compute Cloud (EC2) dan menggunakan PuTTY Gen Terminal Ubuntu sebagai remote access penggunaan protokol jaringan untuk kebutuhan remote server dari kendali jarak jauh.

Keywords:
VPN, VPC, EC2, PuTTY Gen Terminal Ubuntu

ABSTRACT

One of the computer technologies that is commonly used by agencies/companies is the internet network which functions as a bridge to connect between one point to another. Apart from having the advantage of being a medium for long-distance communication, the internet also has a lack of security. One of the weakness found is the internet as a transmission medium for important or confidential data. One effort that can be made to overcome this problem is to build a private network in a public network service, which is often known as a Virtual Private Network (VPN). In this research, the VPN was built by combining a Virtual Private Cloud (VPC) with Elastic Compute Cloud (EC2) and using Ubuntu's Terminal in PuTTY Gen as remote access using network protocols for remote server needs from remote control.

1. INTRODUCTION

Dengan adanya kemajuan teknologi yang pesat pada saat ini menyebabkan pemanfaatan jaringan internet sangat membawa pengaruh yang sangat besar terkait sebagai sebuah media untuk berkomunikasi yang dapat menghubungkan sebuah lokasi dengan lokasi lain yang jaraknya berjauhan. Perkembangan teknologi informasi yang pesat semakin memudahkan manusia dalam memperoleh data dan informasi, khususnya terkait dengan aktifitas-aktifitas yang dilakukan dengan bantuan teknologi jaringan internet tersebut.

Data dan informasi dapat ditransfer dari satu titik ke titik yang lain dengan mudah dengan adanya bantuan jaringan internet. Dengan adanya jaringan internet menyebabkan hilangnya keterbatasan jarak dan waktu dalam berkomunikasi. Jaringan internet memiliki manfaat yang sangat besar bagi manusia. Menjadikan internet sebagai media untuk berkomunikasi dapat mempercepat aktifitas baik dalam bekerja ataupun bertukar informasi. Dengan adanya jaringan internet ini memudahkan manusia untuk mencari maupun menerima informasi dengan cepat. Namun internet juga memiliki sebuah kekurangan khususnya dalam hal tingkat keamanan. Hal ini dikhususkan dalam manfaat jaringan internet sebagai media transmisi data dan informasi yang bersifat penting atau confidential. Banyaknya aktifitas yang dapat kita lakukan di internet tak jarang juga terdapat beberapa konten yang tidak dapat kita akses dan tidak menutup kemungkinan data pribadi kita dapat dicuri melalui internet.

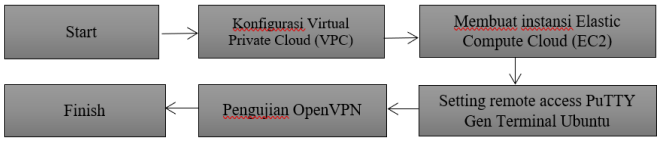
Salah satu upaya yang dapat dilakukan untuk mengatasi permasalahan tersebut adalah dengan membangun sebuah jaringan privasi dalam sebuah layanan jaringan publik, atau yang sering dikenal dengan Virtual Private Network (VPN). VPN adalah sebuah jaringan privasi yang terhubung pada jaringan publik di jaringan internet yang memberikan tingkat keamanan data dan akses global yang lebih privasi atau khusus melalui jaringan internet. VPN berguna agar dapat melewati pembatasan geografis terhadap suatu konten, tidak hanya untuk melewati batasan-batasan tersebut VPN juga berfungsi untuk mengamankan data-data pribadi saat mengakses internet.

Pada penelitian ini VPN dibangun dengan mengkombinasikan Virtual Private Cloud (VPC) dengan Elastic Compute Cloud (EC2) dan menggunakan PuTTY Gen Terminal Ubuntu sebagai remote access penggunaan protokol jaringan untuk kebutuhan remote server yang diakses dari kendali jarak jauh.

2. RESEARCH METHODS

2.1 Framework Penelitian

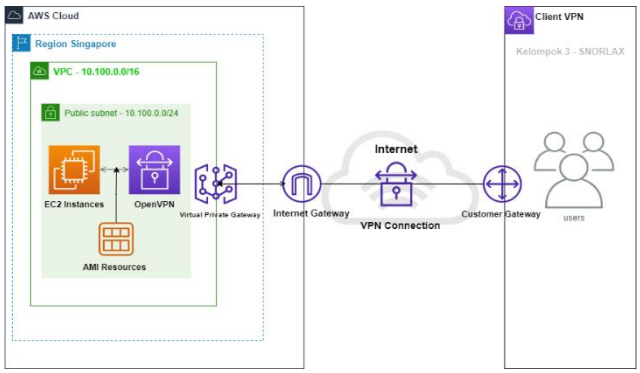
Berikut ini merupakan framework penelitian dari pembuatan VPN dengan kombinasi Virtual Private Cloud (VPC) dengan Elastic Compute Cloud (EC2) dan menggunakan PuTTY Gen Terminal Ubuntu untuk remote access penggunaan protokol jaringan:



Gambar 1. Framework Penelitian

Berdasarkan gambar 1 diatas, penelitian dimulai dengan mengkonfigurasi Virtual Private Cloud (VPC) terlebih dahulu pada langkah pertama. Langkah selanjutnya yaitu membuat atau membangun instansi Elastic Compute Cloud (EC2) yang kemudian dilanjut dengan mengatur pengaturan remote access yang menggunakan PuTTY Gen untuk Terminal Linux Ubuntu. Langkah terakhir dari penelitian ini yaitu melakukan pengujian terhadap OpenVPN yang dibangun.

2.2 Topologi Jaringan



Gambar 2. Topologi Penelitian

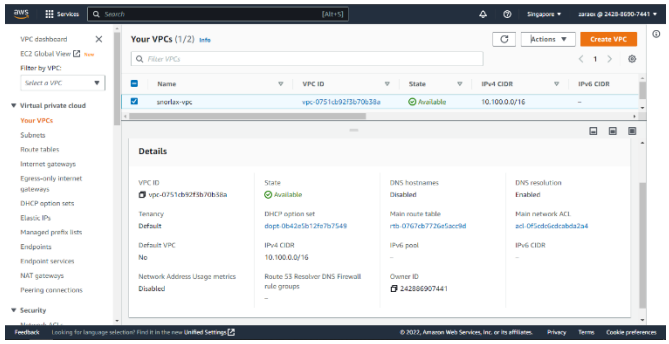
Berdasarkan gambar 2 diatas, sebelum user menjadi client VPN maka user tersebut harus melalui beberapa tahapan proses yang membuat user tersebut menjadi seorang client. Tahapan tersebut adalah dengan melewati Customer Gateway, VPN Connection, Internet Gateway, dan yang terakhir yaitu Virtual Private Cloud (VPC). Dalam penelitian ini, Region yang digunakan dalam konfigurasi VPC adalah Singapore. VPC disetting dengan public subnet ip 10.100.0.0/24. Didalam VPC tersebut juga akan disetting EC2 Instances, AMI Resources, dan OpenVPN. Setelah semua tahapan proses dilewati, maka user tersebut kemudian dikatakan sebagai Client VPN.

3. RESULT AND DISCUSSION

3.1 Konfigurasi Virtual Private Cloud (VPC)

Tahapan pertama dalam penelitian ini yaitu mengkonfigurasi Virtual Private Cloud (VPC). Proses konfigurasi VPC dilakukan dengan menggunakan layanan arsitektur Amazon Web Service (AWS) yang dipaparkan sebagai berikut:

1. Pada layanan AWS, pilih Create VPC.
2. Input Name = snorlax-vpc, VPC ID = vpc-0751cb92f3b70b38a, dan IPv4 CIDR = 10.100.0.0/16. CIDR adalah sebuah mekanisme routing yang bersifat lebih efisien dibandingkan dengan routing manual yakni dengan membagi alamat IP jaringan kedalam kelas-kelas A,B, atau C.



Gambar 3. Pembuatan VPC

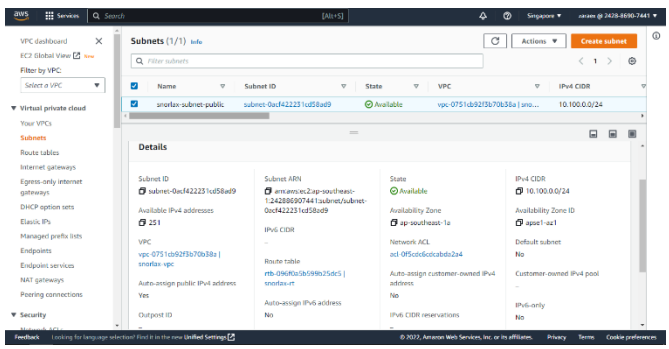
Setelah membuat VPC, langkah selanjutnya yaitu membuat Internet Gateway sebagai jembatan atau alat penghubung yang menghubungkan VPC ke client dan bertanggung jawab untuk meneruskan alir data dari jaringan private ke jaringan public.

Pada tahapan ini dibagian name diisi dengan snorlax-igw dan Internet Gateway ID diisi dengan igw0a55d33d20a24c11b dengan VPC ID yang sama seperti sebelumnya. Lalu Internet Gateway yang telah dikonfigurasi tersebut di Attach ke VPC yang sebelumnya telah dibangun.

Langkah selanjutnya yaitu membuat Route Table atau Tabel Rute. Tabel Rute berisikan seperangkat aturan yang disebut rute yang mengatur aliran jaringan yang berasal dari subnet atau gateway yang ada. Adapun langkah-langkah pengaturan Tabel Rute adalah sebagai berikut:

1. Klik Create Route Table.
2. Pada bagian Routes, isi data Destination = 0.0.0.0/0 untuk aliran jaringan IPv4 dan Target ID Gateway = igw-0a55d33d20a24c11b.
3. Pada bagian Subnet Association, masukkan data Subnet ID = subnet-oacf422231cd58ad9 dan IPv4 CIDR = 10.100.0.0/24.

Langkah terakhir setelah konfigurasi Tabel Rute adalah membuat sebuah subnet dimana IP dari subnet tersebut diambil dari IPv4 CIDR VPC 10.100.0.0.24 dengan subnet ID subnet-0acf422231cd58ad9. Konfigurasi subnet dapat dilihat pada gambar 4 berikut:



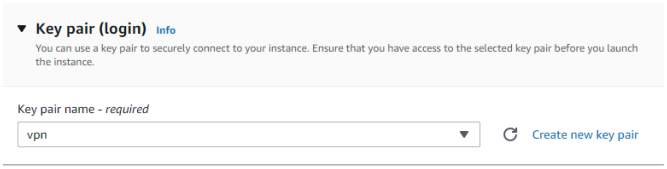
Gambar 4. Konfigurasi Subnet

3.2 Konfigurasi Elastic Compute Cloud (EC2)

Tahapan kedua dalam penelitian ini yaitu membuat instansi EC2. Proses pembuatan instansi EC2 dilakukan dengan langkah-langkah sebagai berikut:

1. Klik Create EC2 Instances.

2. Pada bagian Region, pilih Singapore, isi data Name = snorlax-vpn dengan Instances ID = i-0547e3d1597adf42d, Instance Type = t2.micro dan IP Public = 18.141.138.203.
3. Konfigurasi AMI (Amazon Machine Image) dengan memilih OpenVPN Access Server di bagian list bar.
4. Setelah memilih konfigurasi AMI, langkah selanjutnya adalah dengan membuat Key Pair yang terdiri dari public key dan private key yang akan menghubungkan kredensial keamanan jaringan yang digunakan dengan instansi EC2.

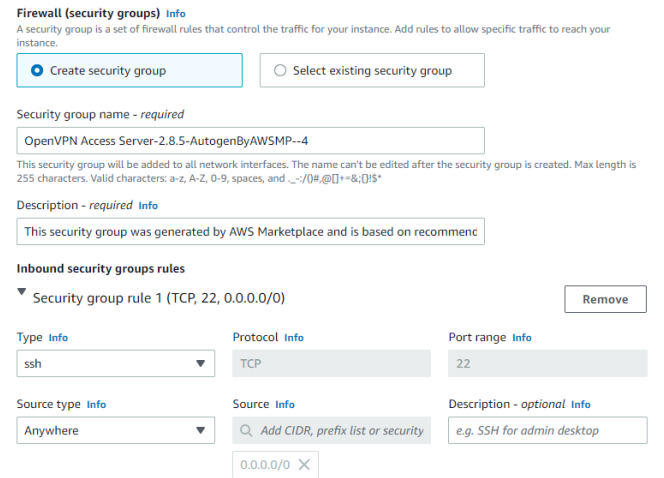


Gambar 5. Key Pairing

5. Langkah selanjutnya adalah mengkonfigurasikan Network agar dapat terhubung dengan Virtual Private Cloud (VPC) dan Subnet yang telah dikonfigurasikan sebelumnya.

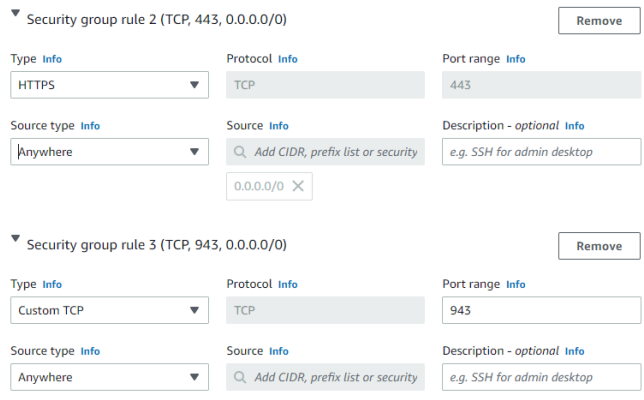
Gambar 6. Konfigurasi Network

6. Setelah menghubungkan konfigurasi Network, atur network settings pada bagian Create Security Group dengan pilihan Security Group Name OpenVPN Access Server-2.8.5-AutogenByAWSMP—4 dengan pengaturan Type menjadi SSH dengan protocol TCP dan port range 22.

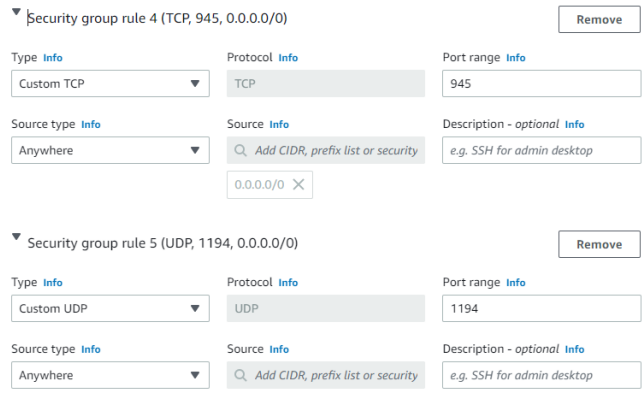


Gambar 7. Network Settings

7. Selanjutnya mengkonfigurasi Security group rule 2 hingga Security group rule 5 seperti gambar berikut ini.

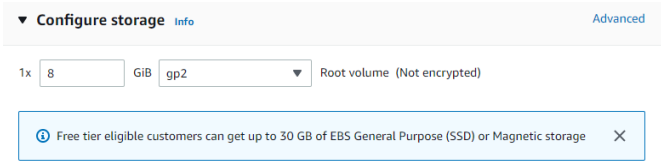


Gambar 8. Security Group Rule 2 dan 3



Gambar 9. Security Group Rule 4 dan 5

8. Langkah terakhir yaitu mengkonfigurasi Storage dengan volume 8 GiB dengan tipe General Purpose SSD (gp2).

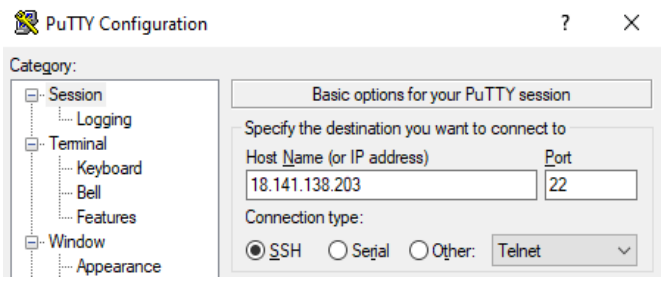


Gambar 10. Konfigurasi Storage

3.3 Konfigurasi remote access dengan PuTTY Gen Terminal Ubuntu

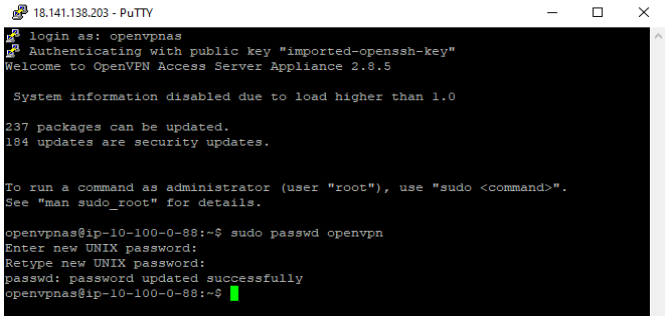
Tahapan selanjutnya setelah mengkonfigurasi instansi EC2 yaitu melakukan pengaturan remote access dengan menggunakan PuTTY Gen Terminal Ubuntu. Langkah-langkah yang dilakukan untuk mengkonfigurasi PuTTY adalah sebagai berikut:

1. Pilih Category Session, pada bagian basic options, masukkan IP Public = 18.141.138.203 dengan Port 22 dan Connection Type sebagai SSH.



Gambar 11. PuTTY Configuration

2. Pilih Category Connection > SSH > Auth, browse file vpn1.ppk yang berada di folder default lalu klik open.
3. Klik Accept, pada menu PuTTY Security Alert, kemudian akan muncul Terminal Ubuntu untuk mengkonfigurasi server EC2 yang telah dibangun sebelumnya.

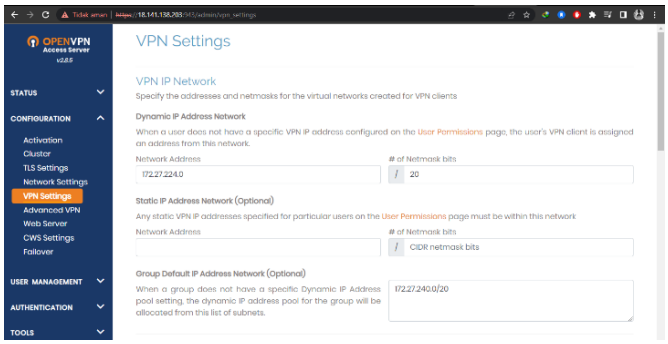


Gambar 12. Konfigurasi PuTTY Terminal Ubuntu

Pada gambar diatas dijelaskan bahwa setelah selesai konfigurasi sebagai root maka selanjutnya kita login sebagai openvpnas untuk membuat user admin dengan perintah "sudo passwd openvpn" dan masukkan password yang kita inginkan untuk login di GUI Admin Login.

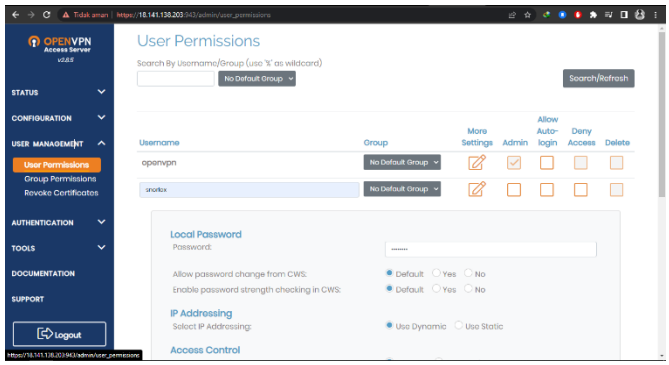
3.4 Hasil Pengujian OpenVPN

Setelah melakukan konfigurasi VPC dan EC2 serta pembuatan user di terminal Ubuntu. Selanjutnya hasil lakukan konfigurasi OpenVPN di alamat yang telah dibangun yaitu htpps://18.141.138.203:943/admin dan login dengan akun user yang telah dibuat sebelumnya dan melakukan pengaturan di bagian VPN Settings.



Gambar 13. Konfigurasi di Terminal Ubuntu PuTTY

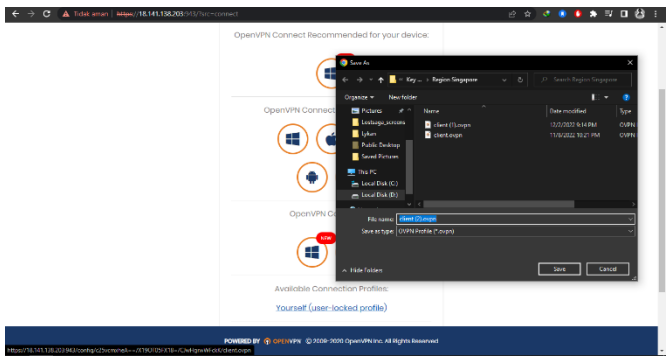
Setelah melakukan pengaturan di bagian VPN Settings, pilih bagian User Management > User Permissions, kemudian atur username dan password untuk user login ke OpenVPN. Pada penelitian ini, username yang digunakan adalah "snorlax" dengan passwordnya, lalu pilih save dan Update Running Server.



Gambar 14. GUI Web Admin User Configuration

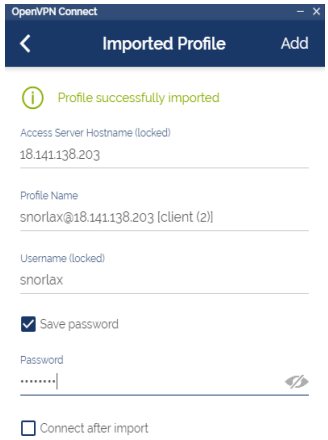
Gambar 15. Update Running Server

Setelah selesai di update, langkah selanjutnya adalah login di alamat https://18.141.138.203:943/ dengan username snolax dan password yang telah dibuat oleh admin sebelumnya. Setelah berhasil login, install software OpenVPN Connect di device yang digunakan dan menyimpan profile user snorlax tersebut di folder yang diinginkan.



Gambar 16. Save Profile Client

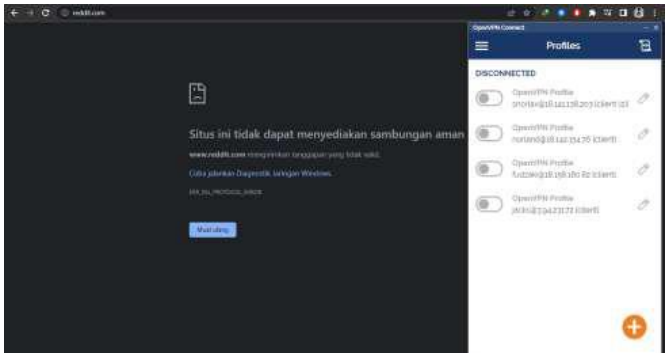
Setelah selesai menginstall dan menyimpan file tersebut, maka langkah selanjutnya adalah import file yang sudah disimpan ke aplikasi OpenVPN Connect lalu isi password akun snorlax dan pilih Add.



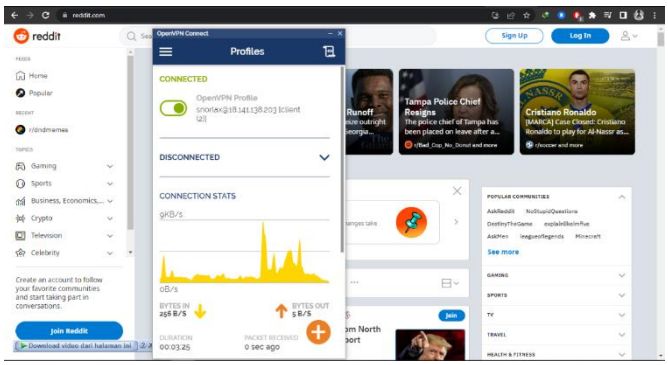
Gambar 17. Add Profile Client

Hasil penelitian yang dilakukan dalam pengujian VPN yang dibangun ini diuji dengan mengakses website yang

diblokir aksesnya di negara Indonesia, yaitu Reddit.com. Berikut merupakan hasil pengujian sebelum dan sesudah menggunakan VPN Snorlax yang dibangun.



Gambar 18. Pengujian akses website yang diblokir 1



Gambar 19. Pengujian akses website yang diblokir 2

4. CONCLUSION

Dari pengujian yang dilakukan dapat ditarik beberapa kesimpulan diantaranya adalah pembuatan VPn sebagai alat yang menjembatani hubungan antara client dan server maupun sebaliknya berhasil dibuat dengan menggunakan kombinasi Virtual Private Cloud (VPC) dan Elastic Compute Cloud (EC2). VPN yang dibangun dapat meningkatkan keamanan aliran data yang berasal dari client kepada server dikarenakan VPN yang dibangun hanya dapat diakses oleh user yang memiliki password sendiri. Dengan kata lain, tidak ada pihak ketiga yang mengetahui aliran data yang mengalir selain user tersebut sehingga privasi lebih terjamin keamanannya dibandingkan dengan menggunakan jaringan internet tanpa VPN ataupun mengunakan VPN konvensional yang banyak beredar di internet.

REFERENCES

[1] Luo Youqiang, et al. 2017. DNS tunnel Trojan detection method based on communication behavior analysis. Journal of Zhejiang University (Engineering Science Edition) 51.9: 1780-1787.

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

[3] Paulus Y.J. 2012. Computer Networking, Pengaturan Jaringan, Keamanan Jaringan, Koneksi dan sharing, Troubleshooting Jaringan. Yogyakarta: Andi.

[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] Retno, S. & Hasdyna, N. 2020. Algoritma Honey Encryption dalam Sistem Pendataan Sertifikat Tanah dan Bangunan di Universitas Malikussaleh. INFORMAL: Informatics Journal, Vol 5, No 3, p. 87 – 95.

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

[7] Supriyanto, B., & Suharyanto, S. (2019). Perancangan Jaringan VPN Menggunakan Metode Point to Point Tunneling Protocol. Jurnal Teknik Komputer, 5(2), 235-240.

[8] 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.

[9] Syafrizal, M. 2008. Pengantar Jaringan Komputer. Yogyakarta : Andi.

[10] Wardoyo, S., Ryadi T., and Fahrizal, R. "Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni dan Tunneling 6 to 4 Berbasis Router Mikrotik," J. Nas. Tek. Elektro, vol. 3, no. 2, p. 106

[11] Setiawan, B., & Aditya, R. (2020). Implementasi VPC dan EC2 dengan Remote Access Menggunakan PuTTY di Ubuntu pada VPN Pribadi. Jurnal Teknologi Informasi dan Komunikasi, 12(2), 87-95. doi:10.19184/jtik.v12i2.10467

[12] Rahmawati, D., & Prasetyo, H. (2021). Manajemen Remote EC2 di VPC Menggunakan PuTTY di Sistem Ubuntu. Jurnal Ilmiah Teknik Informatika, 15(3), 102-110. doi:10.21512/jiti.v15i3.12345

[13] Lestari, E., & Darmawan, A. (2019). Penerapan VPN Pribadi untuk Akses Aman ke EC2 di VPC Menggunakan PuTTY dan Ubuntu. Jurnal Informatika, 8(1), 65-74. doi:10.30591/jti.v8i1.2019

[14] Haryanto, T., & Mulyadi, S. (2022). Konfigurasi VPC dan EC2 dengan Remote Access PuTTY di Ubuntu. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 6(1), 56-64. doi:10.25126/jpttik.v6i1.2022.3211

[15] Nurhayati, S., & Purnomo, E. (2020). Implementasi VPC dan EC2 dengan Akses Remote Menggunakan PuTTY pada VPN Pribadi. Jurnal Rekayasa Sistem dan Teknologi Informasi, 14(2), 98-108. doi:10.21493/jrsti.v14i2.1009.