https://jurnal.pustakagalerimandiri.co.id/index.php/pustakadata
DOI : https://doi.org/10.55382/jurnalpustakadata.v3i1.525

Jurnal Pustaka Data

Pusat Akses Kajian Database, Analisa Teknologi, dan Arsitektur Komputer

Vol. 3 No. 1 (2023) 30 – 36

E ISSN: 2809-7483

Optimalisasi VPN Gate Client pada Wi-Fi Publik untuk Keamanan Transmisi Data dan Akses Internet

Riska Robianto
Sistem Komputer, Fakultas Ilmu Komputer Universitas Putra Indonesia YPTK Padang
riskarobianto@upiyptk.ac.id

Abstract

Currently internet services have become a major need in the midst of society, this is because all affairs are based on digital services (online). In fact, internet services are no longer just the delivery of information but are used as a means of entertainment and socializing on the Social Networking Services (SNS) platform. The government and the private sector are competing to build infrastructure such as public Wireless Fidelity (Wi-Fi) access in several public facilities so that internet access can be enjoyed by the public, wherever and whenever. In fact, this progress is sometimes not in line with government regulations that limit and even block some domestic and global websites with the Government Firewall. On the other hand, the ease of getting free internet service via Public Wi-Fi is used by unauthorized people to then steal personal data by tracking IP addresses, viewing user identities and so on, so that internet activities that should be private are no longer safe. . Or the transmission of data that can be intercepted easily without encryption. For this reason, choosing the right solution to this problem is the author's discussion of this article, which is a step to optimize VPN Gate Client on public Wi-Fi for data transmission security and internet access.

Keywords: data transmission, firewall, public-wifi, VPN gate client, VPN optimization.

Abstrak

Saat ini layaan internet sudah menjadi kebutuhan utama ditengah-tengah masyarakat, hal ini disebabkan semua urusan sudah berbasis layanan digital (online). Bahkan, layanan internet tidak lagi sekedar penyampaian informasi tetapi dimanfaatkan sebagai sarana hiburan dan bersosialisasi di platform Social Networking Services (SNS). Pemerintah maupun swasta berlomba membangun infrastruktur semisal adanya akses Wireless Fidelity (Wi-Fi) publik pada beberapa fasilitas umum sehingga akses internet dapat dinikmati oleh masyarakat, dimanapun dan kapanpun. Faktanya, kemajuan tersebut terkadang tidak sejalan dengan regulasi pemerintah membatasi bahkan memblokir beberapa website domestik maupun global dengan Firewall Pemerintah. Disisi lain, mudahnya mendapatkan layanan internet gratis melalui Wi-Fi Publik tersebut dimanfaatkan oleh orang yang tidak berwenang untuk kemudian mencuri data pribadi dengan melakukan pelacakan terhadap alamat IP, melihat identitas pengguna dan sebagainya, sehingga aktivitas internet yang seharusnya menjadi sebuah privasi tidak lagi menjadi aman. Ataupun terhadap transmisi data yang dapat disadap dengan mudah tanpa adanya enkripsi. Untuk itu, pemilihan solusi yang tepat terhadap persoalan ini menjadi pembahasan penulis dari artikel ini, yaitu diperlukan sebuah langkah optimalisasi VPN Gate Client pada Wi-Fi publik untuk keamanan transmisi data dan akses internet.

Kata kunci: firewall, optimalisasi VPN, transmisi data, VPN gate client, wifi-publik

Submitted : 20-06-2023 | Reviewed : 24-06-2023 | Accepted : 27-06-2023

1. Pendahuluan

Situasi endemic Covid-19 telah merubah paradigma dalam aktivitas harian manusia [1]. Meskipun pembatasan ruang gerak dan waktu untuk bekerja, belajar dan sebagainya tidak lagi dibelakukan secara ketat akan tetapi kebiasaan yang dilakukan selama masa pandemi Covid-19 masih tetap melekat seolah telah menjadi kebiasaan baru (new normal) [2].

Saat ini, layanan internet menjadi kebutuhan utama ditengah-tengah masyarakat. Hal ini disebabkan semua urusan sudah berbasis layanan digital (online) [3]. Bahkan, layanan internet tidak saja sekedar penyampaian informasi tetapi juga dimanfaatkan sebagai sarana hiburan dan bersosialisasi menggunakan berbagai platform media sosial [4].

Internet merupakan jaringan komputer seluruh dunia yang telah ber-evolusi yang memungkinkan setiap individu untuk berkomunikasi satu sama lain dengan komputer dan server tanpa batasan apapun [5]. Setiap situs web yang disediakan oleh perorangan, organisasi, pemerintah ataupun swasta dapat diakses oleh masyarakat, kapanpun, serta dari manapun. Setiap individu di dunia adalah pelanggan potensial dari layanan web tersebut, sehingga tidak sedikit dari perusahaan web berupaya terus mengembangkan dan meningkatkan layanan mereka [6].

Dalam memperluas jangkauan dan layanan internet, pemerintah maupun swasta berlomba membangun infrastruktur semisal adanya akses Wireless Fidelity (Wi-Fi) publik pada beberapa fasilitas umum seperti di perkantoran, sekolah, rumah sakit, bandara, pusat perbelanjaan, dan tempat-tempat lain. Hal ini mendorong mobilitas pengguna yang tinggi karena dapat menikmati layanan internet di area Wi-Fi publik tersebut tanpa harus menggunakan kabel [7].

Internet menyediakan ketersedian informasi dan layanan apa saja tanpa adanya pembatasan akses terhadap web tertentu. Namun, di beberapa negara tidak mengizinkan rakyatnya mengakses situs web tertentu bahkan sengaja memblokir situs web yang dianggap tidak sesuai dengan regulasi pemerintah. Misalnya, situs berbagi video seperti YouTube, atau situs Social Networking Service (SNS) seperti Twitter atau Facebook. Pemerintah menerapkan filter yang biasa disebut Firewal [8].

Terkadang Firewall pemerintah memaksa orang untuk hanya menggunakan layanan web dalam negeri (domestic) daripada yang tersedia di seluruh dunia. Di bawah kendali dan pengawasan tersebut, orang tidak dapat mengakses layanan web global yang menyuguhkan informasi dan layanan menarik sesuai dengan keinginan mereka [9]. Dengan kata lain, regulasi seperti itu memberikan kerugian kepada beberapa penyedia layanan web domestic. Pada akhirnya, proteksi berlebihan pemerintah tersebut akan menyebabkan penurunan kepentingan publik, terkekangnya kebebasan rakyat untuk berekspresi serta bersosialisasi karena kebanyakan orang di negara tersebut dijauhkan dari layanan web yang berharga di seluruh dunia [10].

Selain Firewall yang diberlakukan di beberapa negera, ada sisi lain yang tidak diketahui oleh sebagian pengguna (user) akan risiko dan kerugian dalam menggunakan layanan internet. Misalnya IP Address yang dapat dilacak untuk suatu kepentingan oleh pihak tertentu sehingga bocornya informasi atau identitas melalui log server yang disimpan oleh Internet Service Provider (ISP) [11].

Risiko lainnya adalah sebagian besar jaringan Wi-Fi publik (nirkabel) rentan terhadap packet sniffing sehingga dapat disadap oleh siapa saja yang tidak bertanggungjawab karena biasanya tidak terenkripsi. Selain itu, administrator jaringan atau pemilik fasilitas memiliki kesempatan untuk memanfaatkan komunikasi yang dilakukan. Bahkan jika terhubung ke internet di rumah sekalipun, ada risiko bahwa karyawan ISP atau perusahaan telekomunikasi mungkin melakukan penyadapan untuk mengamati paket teks biasa tanpa disadari [12].

Penelitian sebelumnya juga telah dilakukan oleh Hidayat S [13] yaitu mengoptimalkan RouterOS yang dimiliki perusahaan agar dapat menjadi jaringan Tunnel yang dapat menjembatani komunikasi data antara jaringan publik (internet) dengan jaringan LAN kantor, sehingga karyawan dapat mengakses resource kantor tanpa batasan ruang dan waktu akibat regulasi pemerintah dan kebijakan perusahaan. Penelitian lain yang dilakukan oleh M Noviansyah [14] juga menerapkan VPN Tunnel untuk mencegah Packet Sniffing dengan metode LP2TP/IPSec. Untuk mengamankan paket data yang dikirim digunakan IPSec, sedangkan dengan IPSec VPN proses pengiriman data akan lebih aman tanpa adanya gangguan karena data yang telah dikirim telah dienkripsi dengan baik.

Pada penelitian yang dilakukan oleh R Andriani [15] yaitu mengimplementasikan VPN pada Proxy Router dengan metode Point to Point Tunneling Protocol (PPTP) sehingga karyawan tetap dapat mengakses jaringan lokal kantor dari jaringan eksternal dengan aman dan lancar, dimana sebelum menerapkan server VPN keamanan dalam akses internet masih rentan terhadap penyadapan dan serangan, baik informasi berupa login halaman website, login router, maupun informasi saat transmisi data sangat mudah didapatkan. Sangat berbeda, ketika user menggunakan koneksi server VPN tindakan tersebut tidak dapat dilakukan lagi, dengan metode Point to Point Tunneling Protocol

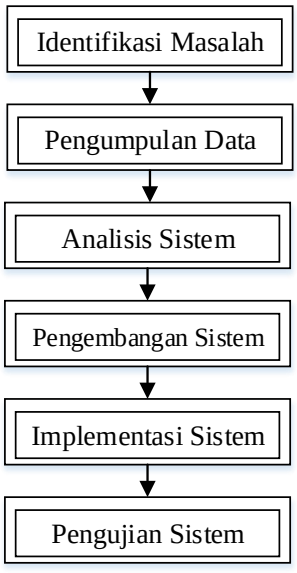
Submitted : 20-06-2023 | Reviewed : 24-06-2023 | Accepted : 27-06-2023

(PPTP) karyawan yang bekerja secara Work From Home (WFH) dapat saling terhubung dengan baik.

Pemilihan solusi yang tepat terhadap persoalan di atas menjadi tujuan dan pembahasan penulis dalam artikel ini, yaitu diperlukan sebuah langkah optimalisasi VPN Gate Client pada Wi-Fi publik untuk keamanan transmisi data dan akses internet [16]. Sehingga user tidak dirugikan oleh regulasi pemerintah, pelacakan alamat IP dan penyusupan dalam akses internet. Hal ini dapat menjamin hak user serta memberikan rasa aman dan nyaman dalam beraktivitas secara online.

2. Metode Penelitian

Adapun tujuan dari metode penelitian secara umum adalah untuk memperoleh pengetahuan baru serta penemuan baru berbekal pengetahuan dan penemuan-penemuan terdahulu. Selain itu dengan metode penelitian ini juga untuk membuktikan atau menguji kebenaran dari suatu ilmu yang telah ada kebenarannya. Tujuan lain dari metode penelitian adalah agar dapat melakukan pengembangan ilmu-ilmu ataupun hasil dari penemuan yang sudah ada untuk kemaslahan umat. Kerangka penelitian merupakan konsep atau tahapan-tahapan yang diurutkan secara sistematis dan dilakukan pada penelitian seperti yang akan diuraikan pada Gambar 1.



Gambar 1. Kerangka Penelitian

Tahapan penelitian ini diawali dengan mengidentifikasi masalah sampai pada implementasi sistem yang dijelaskan dibawah ini:

2.1 Identifikasi Masalah.
Beberapa masalah yang dapat diidentifkasi dari uraian pendahuluan diatas diantaranya adalah 1) firewall pemerintah memblokir akses ke situs web tertentu. 2) Dimungkinkan untuk mengidentifikasi individu dengan menelusuri alamat IP yang seharusnya ditemukan di *log server*. 3) Jaringan nirkabel publik rentan terhadap packet sniffing.

2.2 Pengumpulkan Data.
Merupakan metode dimana penelitian memperoleh data yang dibutuhkan melalui penelitian kepustakaan dan observasi. Kepustakaan adalah adalah memahami literatur untuk menyelesaikan permasalahan dalam penelitian. Adapun observasi merupakan cara pengumpulan data secara langsung melalui pengamatan ditempat terhadap target penelitian.

2.3 Analisis Sistem.
Pada tahap ini merupakan fase awal dari pengembangan sistem. Analisis sistem merupakan cara penyelesaian masalah yang menjabarkan bagian-bagian komponen dengan mempelajari sejauh mana bagian-bagian komponen tersebut bekerja dan berinteraksi dengan komponen lainnya untuk mencapai tujuan.

2.4 Pengembangan Sistem.
Pengembangan sistem merupakan penentuan dalam menyusun sistem yang baru untuk merubah atau menggantikan sistem yang lama baik sebagian maupun secara keseluruhan. Pada tahap ini sistem yang telah ada digantikan dengan penggunaan VPN Gate Client.

2.5 Implementasi Sistem.
Implementasi merupakan tahap dalam menerapkan sistem yang baru berpedoman pada hasil analisa serta perancangan pada tahap sebelumnya. Aksi dari tahapan ini adalah implementasi langsung pada Wifi publik dengan client menggunakan sistem operasi Microsoft Windows.

2.6 Pengujian Sistem
Untuk memperoleh hasil akhir dari rangkaian penelitian ini dilakukan pengujian menggunakan perangkat lunak (*software*) SofEther VPN pada sistem operasi Microsoft Windows.

3. Hasil dan Pembahasan

Hasil evaluasi didapat dari pengembangan sistem yang dilakukan yaitu dengan membuat rancangan sistem yang baru untuk merubah atau menggantikan sistem yang sebelumnya, disini memanfaatkan layanan online VPN Gate Client. Tujuan dari VPN Gate Cient ini adalah untuk mencarikan solusi terhadap permasalahan yang telah dikemukan diatas serta memperluas pengetahuan tentang "Server Relay VPN Publik Terdistribusi Global". VPN Gate Client adalah gratis tidak diperlukan pendaftaran tunggal, dan menerima koneksi anonim. VPN Gate Client mendukung berbagai sistem operasi mobile dan

desktop serta mendukung berbagai VPN Transport Protokol. Diuraikan pada Tabel 1.

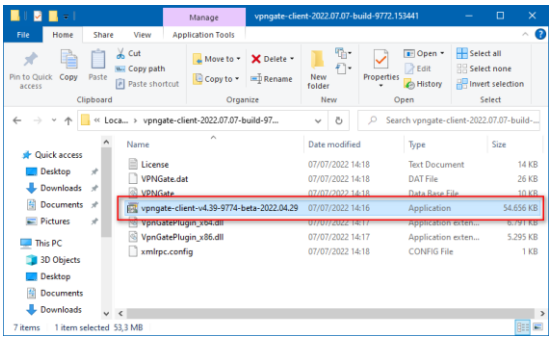
Kelebihan lain dari VPN Gate client adalah setiap *server* VPN memiliki *IP Address dinamis* (DHCP). Sehingga IP Address dapat berubah pada periode acak. Oleh karena itu, *IP Address* sewaktu-waktu dapat saja terputus dari *server* VPN. Kemudian semua *server* VPN mampu mengarahkan lalu lintas (traffic) *user* ke internet, sehingga dapat menyembunyikan atau menyamarkan IP Address dari negara asal. Menggunakan *server* yang berada pada lokasi tertentu selain wilayah *user* dapat memberikan kemudahan dalam mengakses beberapa halaman website, karena lalu lintas jaringan akan terpantau seakan berasal dari negara tempat *server* VPN berada. Berikut tabel protokol VPN untuk terhubung ke VPN Gate Windows.

Tabel 1. protokol VPN untuk terhubung ke VPN Gate di Windows.

Karakteristik	SoftEther VPN (SSL-VPN)	L2TP/IPSEC	OpenVPN	MS-SSTP
Protokol Transportasi VPN	HTTPS (TC/IP) dan UDP Hibrida	IPsec	Protokol Asli (TCP, UDP)	HTTPS (TCP/IP)
Throughput	Cepat	Cepat	Lambat	Lambat
Fungsi Daftar Server Relay Gerbang VPN	✓	-	-	-
Konfigurasi Mudah	✓	✓	-	✓
Kompatibel dengan proksi HTTP	✓	-	✓	✓
Kompatibel dengan SOCKS Proxy	✓	-	✓	✓
Lewati Firewall yang Dibatasi (dengan Menggunakan SSL Murni)	✓	-	-	✓
Dioptimalkan untuk Melewati Firewall Pemerintah	✓	-	-	-
Perangkat Lunak Klien Terpasang dalam Sistem Operasi	-	✓	-	✓
Sistem Operasi yang Kompatibel	Windows 98 SE, ME, 2000, XP, 7, 8, 10, Server 2003, 2008, 2012	Windows XP, 7, 8, 10, RT, Server 2003, 2008, 2012	Windows 2000, XP, 7, 8, 10, Server 2003, 2008, 2012	Windows 7, 8, 10, RT, Server 2003, 2008, 2012

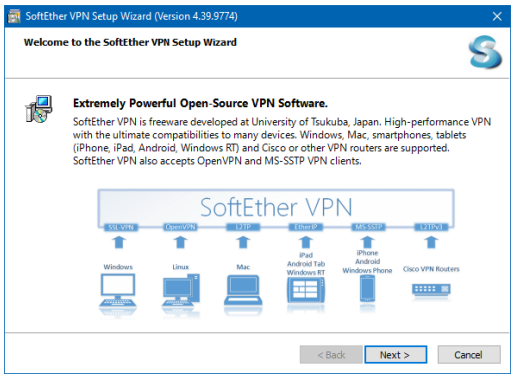
[Sumber: https://www.vpngate.net/en/howto_windows.aspx]

Setelah mengetahui beberapa protokol yang terdapat pada VPN, selanjutnya dilakukan tahap implementasi dengan cara meng-unduh software VPN Gate Client pada situs resminya. Unduh SoftEther VPN Client khususnya veris "Plugin VPN Gate Client". Berikutnya ekstrak file konten ZIP, dan pilih file aplikasi (exe) yang namanya dimulai dengan "vpngate-client", jalankan file setup dilanjutkan dengan tahap instalasi.

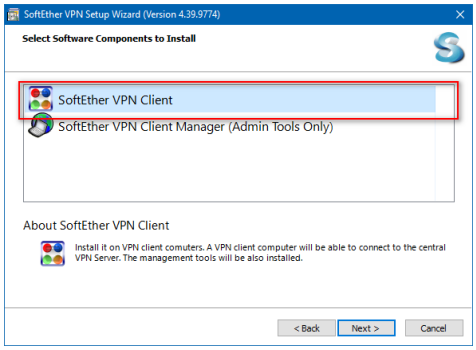


Gambar 2. Hasil Ekstrak konten file Zip yang di Unduh

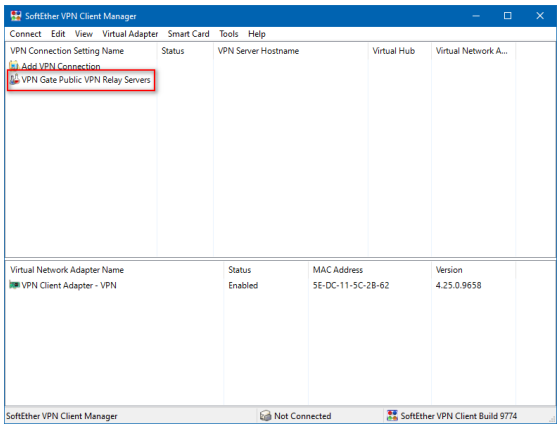
Pada Gambar 2 dijelaskan bahwa untuk instal vpngate-client harus diekstrak file setup dan beberapa file DLL lainnya terlebihdahulu.



Gambar 3. Instalasi file Setup SoftEther VPN

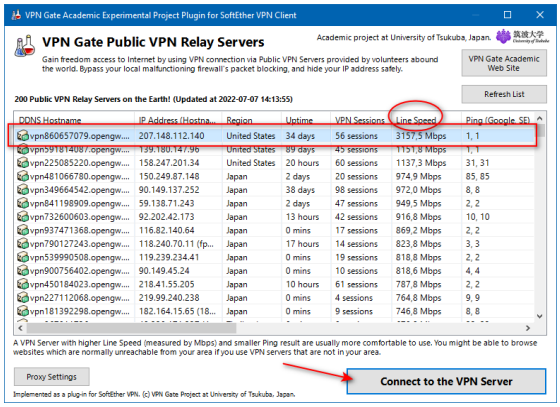


Gambar 4. Pemilihan Komponen Perangkat Lunak untuk di Instal



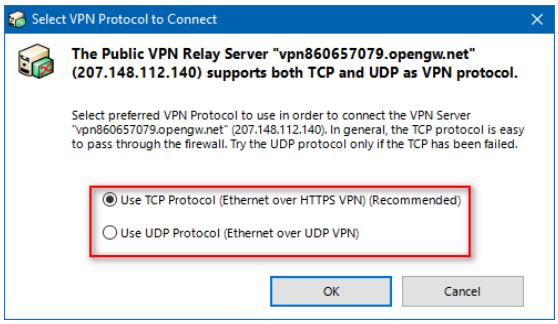
Gambar 5. SoftEther VPN Client Manager

Pada Gambar 5 di atas dapat memiih VPN Gate Public VPN Relay Server dari seluruh dunia oleh sukarelawan yang menyediakan akses ke *server* mereka secara gratis tanpa diperlukan pendaftaran tunggal.

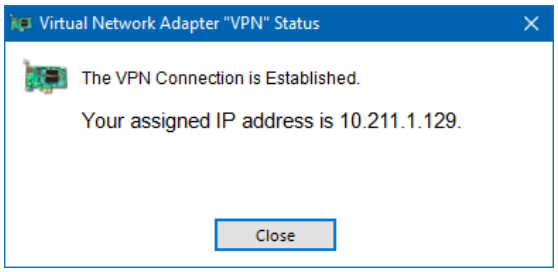


Gambar 6. SoftEther VPN Client Manager

Dari Gambar 6 di atas dapat dilihat daftar dari *server* VPN Gate Public yang sedang berjalan. *Server* VPN Gate Public tersebut dapat dipilih dengan memperhatikan beberapa keterangan yang bisa dijadikan pertimbangan dalam menentukan *server* VPN, diantaranya adalah: IP Address, Region, Uptime, VPN Sessions, Line Speed, Ping, SSL-VPN (TCP), UDP Support, Logging Policy, Cumulative Transfers, Operator Name, Operator's Message, Total Score.



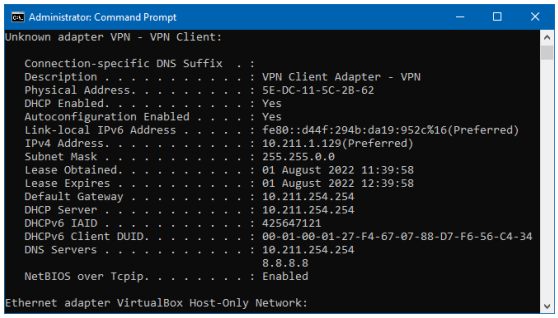
Gambar 7. Pemilihan Protokol VPN (TCP atau UDP)



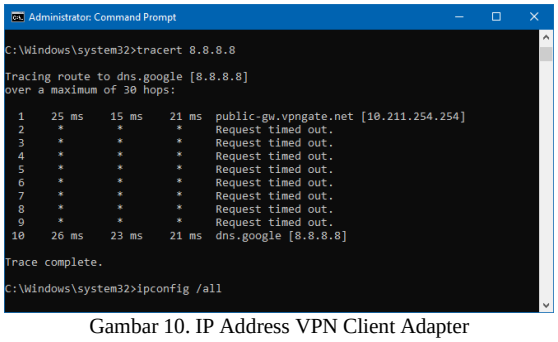
Gambar 8. Status VPN Adapter

Dari Gambar 8 di atas dapat dijelaskan, jika koneksi VPN berhasil dilakukan maka akan muncul pesan seperti jendela di atas. Namun jika koneksi gagal dihubungkan ke *server* VPN tertentu, maka dapat mencoba kembali dengan memilih *server* VPN yang lain. Agar koneksi berjalan dengan baik perhatikan juga *uptime*, *line speed* dan *ping* google seperti pada Gambar 6 sebelumnya.

Langkah berikutnya adalah tahap pengujian dengan cara melakukan rute pelacakan (*tracert*) ke Google Publik DNS untuk melihat keberhasilan dari penggunaan perangkat lunak (*software*) VPN tersebut. Saat koneksi VPN dibuat, Adaptor Jaringan Virtual di sistem operasi Windows akan dibuat dan diberi *IP Address* yang dimulai dengan "10.211.". Alamat default gateway akan ditetapkan pada Adaptor Jaringan Virtual. Ketikkan "ipconfig /all" pada command prompt Windows untuk mengkonfirmasi konfigurasi jaringan serta ketikan "tracert 8.8.8.8" untuk melacak lintasan yang diambil paket protokol internet (IP).



Gambar 9. IP Address (10.211.) VPN Client Adapter

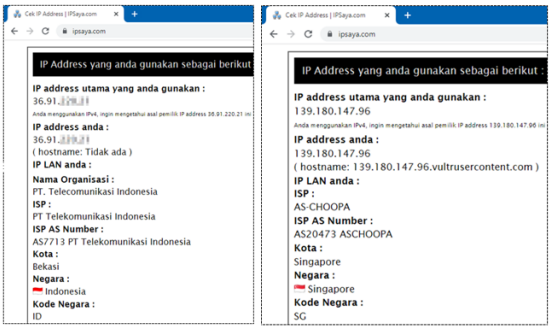


Gambar 10. IP Address VPN Client Adapter

Seperti pada Gambar 10 di atas, jika jalur paket melalui "10.211.254.254", komunikasi internet

sekarang diteruskan melalui salah satu *server* VPN Gate Public.

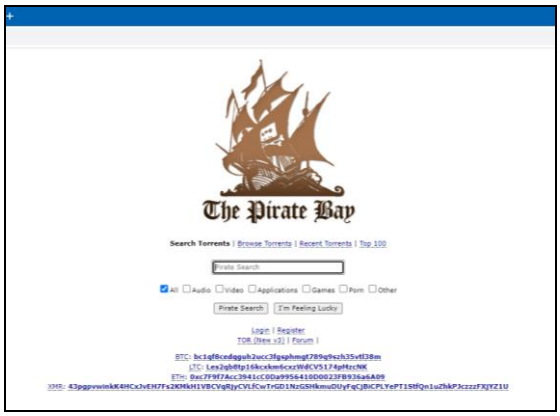
Pengujian berikutnya adalah dengan mengunjungi halaman https://ipsaya.com/ untuk melihat alamat IP global pada perangkat saat ini. Disini terlihat negara atau wilayah sumber telah diubah ke negara lain jika terhubung ke *server* VPN yang terletak di negara luar negeri.



Gambar 11. IP Address dan Negara Asal (a) Perubahan IP Address dan Negara Asal (VPN) (b)

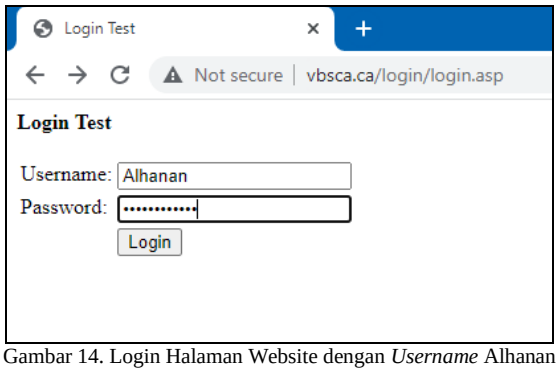
Pengujian berikutnya adalah dengan mengakses beberapa halaman website yang terindikasi telah diblokir oleh Kominfo.

Gambar 12. Halaman Website yang Diblokir Kominfo

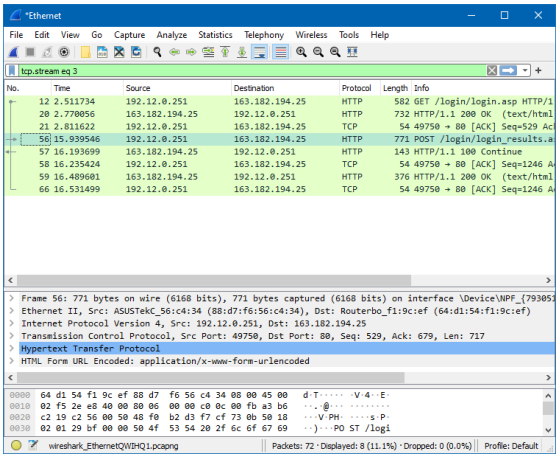


Gambar 13. Halaman Website yang Diblokir Kominfo Dapat Diakses dengan Mudah

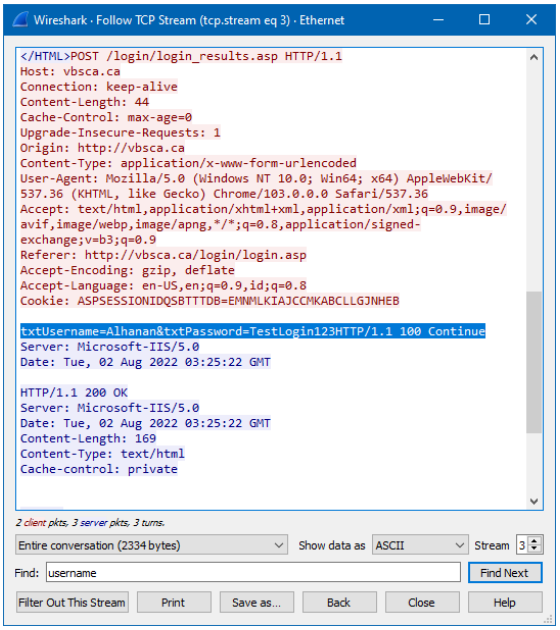
Pengujian akhir adalah dengan menggunakan perangkat lunak (The *Wireshark Network Analyzzer*) untuk simulasi penyadapan melalui protokol HTTP. Langkah awal akses halaman Website http://vbsca.ca/login/login.asp dan masukan *username* dan *password* untuk kemudian akan di tangkap (*capture*) menggunakan TCP Stream.



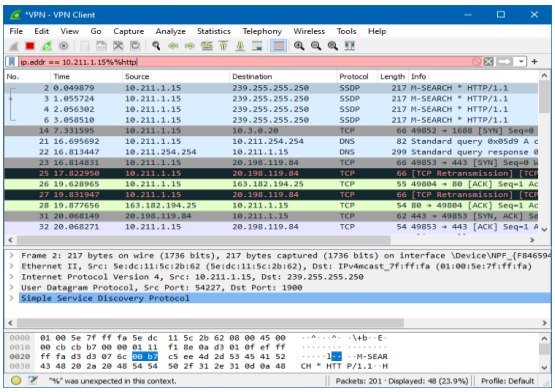
Gambar 14. Login Halaman Website dengan *Username* Alhanan dan *Password* TestLogin123



Gambar 15. Proses *Capturing Username* dan *Password* Login



Gambar 16. *Capturing Username* dan *Password* Login yang Didapatkan



Gambar 17. *Capturing Username* dan *Password* Login Gagal Menggunakan VPN Gate Client

4. Kesimpulan

Setelah serangkain penelitian dilakukan, terutama dari hasil implementasi dan pengujian pada sistem yang baru, pada perangkat yang menggunakan VPN Gate Client maka didapatkan hasil dimana terhadap halaman website yang diblokir oleh firewall pemerintah maupun halaman website global dapat diakses dengan mudah tanpa hambatan seperti ditujukkan pada Gambar 12 dan Gambar 13. Berikutnya terhadap IP Address dapat disamarkan dan identitas dapat disembunyikan ketika berselancar di internet sehingga aktivitas lebih aman dan privasi dapat terlindungi seperti ditujukkan pada Gambar 11 (a) dan (b). Adapun terhadap packet sniffing transmisi data atau paket data yang dikirim melalui jaringan dapat terbebas dari penyadapan karena setiap paket data telah terenkripsi seperti ditunjukkan pada Gambar 15, Gambar 16 dan Gambar 17. Penelitian ini dapat dikatakan berhasil dengan baik sesuai dengan tujuan dan harapan, untuk penelitian berikutnya disarankan mencoba WireGuard yaitu VPN yang sederhana namun cepat dan modern banyak digunakan di dunia industri karena menggunakan kriptografi canggih.

Daftar Rujukan

[1]. Venkatapuram, S. (2020). Human capabilities and pandemics. *Journal of Human Development and Capabilities*, *21*(3), 280-286. DOI: https://doi.org/10.1080/19452829.2020.1786028

[2]. Alraouf, A. A. (2021). The new normal or the forgotten normal: contesting COVID-19 impact on contemporary architecture and urbanism. *Archnet-IJAR: International Journal of Architectural Research*. DOI: https://doi.org/10.1108/ARCH-10-2020-0249

[3]. Freddy, H. T. R., Achmad, W., & Nasution, M. S. (2022). The Effectivity Of Public Services Based On Smart Goverment In Bukit Raya Distric Pekanbaru City. *Journal of Governance*, *7*(1), 239-259. DOI: http://dx.doi.org/10.31506/jog.v7i1.14557

[4]. Carlson, J. R., Hanson, S., Pancras, J., Ross Jr, W. T., & Rousseau-Anderson, J. (2022). Social media advertising: How online motivations and congruency influence perceptions of trust. *Journal of Consumer Behaviour*, *21*(2), 197-213. DOI: https://doi.org/10.1002/cb.1989

[5]. Bailey, J. (2022). Communication: Telephone, Computers and WWW. In *Inventive Geniuses Who Changed the World* (pp. 363-401). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-81381-9_15

[6]. Fan, C., Hook, L. S., Ibrahim, S., & Ahmad, M. N. (2022). Web Service Applications and Consumer Environments Based on ICT-Driven Optimization. *Journal of Sensors*, *2022*. DOI: https://doi.org/10.1155/2022/5639309

[7]. Hadi, S., & Pangestu, A. Sistem Kantor Pintar Berbasis Internet of Things. DOI: https://doi.org/10.32520/stmsi.v11i2.1745

[8]. Lin, Y. (2022). Social media for collaborative planning: A typology of support functions and challenges. *Cities*, *125*, 103641. DOI: https://doi.org/10.1016/j.cities.2022.103641

[9]. Kawerau, L., Weidmann, N. B., & Dainotti, A. (2022). Attack or Block? Repertoires of Digital Censorship in Autocracies. *Journal of Information Technology & Politics*, 1-14. https://doi.org/10.1080/19331681.2022.2037118

[10]. Nugraha, Y., & Martin, A. (2022). Cybersecurity service level agreements: understanding government data confidentiality requirements. *Journal of Cybersecurity*, *8*(1), tyac004. DOI: https://doi.org/10.1093/cybsec/tyac004

[11]. Singh, S. P., Rao, A. N., & Gupta, T. R. (2021). Real-Time Security Monitoring System Using Applications Log Data. Intelligent Sustainable Systems: Proceedings of ICISS 2021, 213, 375. DOI: https://doi.org/10.1007/978-981-16-2422-3_30

[12]. Fatimah, F., Mary, T., & Pernanda, A. Y. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat. JURTEII: Jurnal Teknologi Informasi, 1(2), 7-11. DOI: http://dx.doi.org/10.22202/jurteii.2022.5707

[13]. Hidayat, S., Budiman, T., & Rini, A. S. (2022). Optimalisasi jaringan tunnel menggunakan routeros untuk mendukung kelangsungan operasional PT. KLK Agriservindo di masa pandemik Covid-19. *Jurnal Sains dan Teknologi Widyaloka*, *1*(1), 1-14. https://doi.org/10.54593/jstekwid.v1i1.44

[14]. Noviansyah, M., & Saiyar, H. (2021). Pencegahan Packet Sniffing Menggunakan Metode VPN Tunnel Untuk Keamanan Jaringan Komputer Berbasis Mikrotik. *Jurnal Akrab Juara*, *6*(4), 36-46.

[15]. Andriani, R., Sa'di, A., & Putra, A. D. (2022). Implementasi VPN Menggunakan Metode Point to Point Tunneling Protocol. *Building of Informatics, Technology and Science (BITS)*, *4*(1), 184-190. https://doi.org/10.47065/bits.v4i1.1611

[16]. Hoang, N. P., Polychronakis, M., & Gill, P. (2022, March). Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. In International Conference on Passive and Active Network Measurement (pp. 518-536). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-98785-5_23