JURNAL ILMIAH INFORMATIKA GLOBAL
VOLUME 13 Nomor 02 Agustus 2022
e-ISSN 2477-3786* | *p-ISSN 2302-500X
DOI : 10.36982/jiig.v13i2.2308

Implementasi Keamanan Akses Terhadap Website Menggunakan *Wireguard* VPN Di Routerboard Mikrotik

Dian Novianto[1)], Yohanes Setiawan Japriadi[2)], Lukas Tommy[3)]

[1), 2), 3)] Program Studi Teknik Informatika, ISB Atma Luhur
Jl. Jendral Sudirman No.Kel, Selindung Baru, Kec. Pangkal Balam, Kota Pangkal Pinang, Kepulauan Bangka Belitung
Email : diannovianto@atmaluhur.ac.id[1)], ysetiawanj@atmaluhur.ac.id[2)], lukastommy@atmaluhur.ac.id[3)]

ABSTRACT

The need for the availability of information is currently very high, especially in the conditions of the COVID-19 pandemic, all organizational activities are carried out online. Human dependence on the role of information technology is increasing and this has consequences for long distance communication between devices, which requires users to be authenticated for access rights granted by the system. The problem that arises is the security of data travel during the authentication process, where there is the possibility of leaking account information. This is because communication is done on a public network while accessing resources that require privacy. Therefore we need a network connection that is safe and efficient. Virtual Private Network (VPN) is a network communication technology that allows you to connect to public networks safely and quickly. The VPN used in the solution to this problem is Wireguard. Wireguard is a VPN protocol built with advanced cryptography and makes it extremely fast and secure. The method used by the author in developing this system is PPDIOO which consists of, Prepare, Plan, Design, Implement, Operate, and Optimize. And also some supporting tools for the development of the system Unified Modeling Language. By using Wireguard VPN, the expected result is the security of the data sent to be more secure and can connect two remote networks privately using the public internet.

Keywords : *VPN, Wireguard, Mikrotik*

ABSTRAK

Kebutuhan akan ketersediaan informasi saat ini sangat tinggi, terlebih di kondisi pandemi covid 19 semua kegiatan organisasi dilakukan secara daring. Ketergantungan manusia akan peranan teknologi informasi semakin meningkat dan hal tersebut mempunyai konsekuensi komunikasi jarak jauh antar perangkat, yang mengharuskan pengguna di authentikasi untuk hak akses yang diberikan oleh sistem. Permasalahan yang timbul adalah keamanan dalam perjalanan data saat proses authentikasi, dimana ada kemungkinan informasi akun yang bocor. Hal ini dikarenakan komunikasi dilakukan di jaringan publik saat sedang mengakses sumber daya yang membutuhkan privasi. Oleh karena itu dibutuhkan sebuah koneksi jaringan yang aman dan efesien. Virtual Private Network (VPN) adalah sebuah teknologi komunikasi jaringan yang memungkinkan untuk dapat terkoneksi ke jaringan publik secara aman dan cepat. VPN yang digunakan dalam solusi permasalahan ini yaitu Wireguard. Wireguard merupakan protokol VPN yang dibangun dengan kriptografi canggih dan membuatnya sangat cepat dan aman. Metode yang digunakan penulis dalam pengembangan sistem ini adalah PPDIOO yang terdiri dari, Prepare, Plan, Design,Implement, Operate, dan Optimize. Dan juga beberapa tools pendukung untuk pengembangan sistem tersebut Unified Modelling Language. Dengan menggunakan Wireguard VPN hasil yang diharapkan adalah keamanan data yang dikirim menjadi lebih aman dan bisa menghubungkan dua jaringan jarak jauh scara private menggunakan internet publik.

Kata Kunci : *VPN, Wireguard, Mikrotik*

Article History
Received : 19/05/2022
Revised : 20/06/2022
Accepted : 02/07/2022
Online : 01/08/2022

1. Pendahuluan

Keamanan hak akses terhadap sebuah sumber daya merupakan faktor yang sangat penting dalam dunia teknologi informasi. Saat ini belum banyak instansi atau organisasi yang sangat konsen terhadap masalah keamanan di jaringan. Tetapi ketika sebuah sumber daya dalam hal ini *server* mendapat serangan melalui jaringan dan terjadi kerusakan sistem, sehingga banyak biaya yang harus dikeluarkan untuk melakukan perbaikan sistem, barulah sebuah instansi atau organisasi bergerak untuk lebih konsen terhadap masalah keamanan sistem. Untuk itu sudah selayaknya investasi dibidang keamanan lebih diperhatikan, untuk mencegah dari pencurian data, dan dari ancaman serangan yang sering terjadi. Terlebih lagi saat komputer *server* terhubung dengan internet maka kemungkinan serangan pun akan semakin meningkat.

Salah satu permasalahan yang biasanya terjadi adalah masalah hak akses terhadap sebuah sistem, akun yang bocor dapat disalahgunakan oleh orang yang tidak berwenang dalam mengakses sebuah sumber daya. Kebocoran akun berupa *username* dan *password* dapat terjadi karena adanya tindakan sniffing, ditambah tidak adanya kombinasi untuk keamanan authentikasi di jaringan. Maka akun tersebut dengan sangat mudah digunakan oleh orang lain. Penerapan metode authentikasi tentunya perlu dikombinasikan dengan metode lain di jaringan agar sistem dapat benar – benar menjamin kemanan hak akses tersebut. Oleh karena itu dibutuhkan suatu mekanisme di jaringan yang dapat mencegah ancaman yang mungkin terjadi secara lebih optimal, salah satu caranya dengan memanfaatkan *virtual private network* (VPN).

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam kantor atau network itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik (Irawan, 2014). Karena VPN memungkinkan untuk melakukan akses informasi di dalam internet secara lebih aman seperti pada saat melakukan *browsing, surfing*, serta kegiatan lainnya. Menggunakan VPN dapat dikatakan lebih aman karena data yang dikirimkan akan dienkripsi lebih dahulu sehingga tetap rahasia meskipun data tersebut dikirim melalui jaringan publik. VPN bekerja dengan cara seolah-olah membuat sebuah jaringan baru di dalam jaringan yang sudah ada atau biasa disebut *tunnel* (terowongan). *Tunneling* ini digunakan untuk membuat jalur *private* dengan menggunakan infrastruktur pihak ketiga. VPN sendiri menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: PPTP, L2TP, dan *Internet Protocol Security* (IPSec). Salah satu layanan VPN yang terdapat pada mikrotik yang dapat dimanfaatkan adalah *wireguard* VPN.

Wireguard adalah salah satu tipe VPN yang sederhana namun cepat , aman dan modern. Saat ini *wireguard* juga sudah mendukung *cross platform* (Linux, windows, macOS, BSD, iOS, dan Android). *Wireguard* tidak mengenal yang namanya *server* dan *client* karena *Wireguard* menggunakan konsep peer (saling berhubungan) (mikrotik.co.id, 2021).

Model pengembangan jaringan yang digunakan dalam penelitian ini adalah PPDIOO (*Prepare, Plan, Design, Implement, Operate, and Optimize*). PPDIOO adalah metode perancangan dan pengembangan jaringan yang di kembangkan oleh Cisco (Imam, 2017). Dengan metodologi ini akan memberikan langkah-langkah kunci untuk keberhasilan perancangan jaringan tersebut (Dian, 2020).

Manfaat dari penelitian ini nantinya dapat menghasilkan sebuah kombinasi pengamanan terhadap akses ke sebuah sumber daya dibidang teknologi informasi yang diakses melalui jaringan publik akan tetapi tetap memberikan keamanan yang ketat.

A. Metode Penelitian

Metode yang digunakan dalam penelitian ini menggunakan metode kualitatif dimana peneliti menjadi alat utama dalam pengumpulan data (Dian, 2018). Pengumpulan data yang dilakukan adalah dengan mengumpulkan referensi yang terkait dengan topik penelitian baik dari jurnal maupun dari buku. Karena dengan cara ini peneliti dapat memahami konsep dari VPN terutama cara kerja dari *wireguard*, sehingga diharapkan dalam pengembangan mekanisme kombinasi keamanan jaringan antara VPN dan authentikasi nantinya akan berjalan dengan baik.

Dalam pengembangan sistem keamanan ini model yang digunakan *PPDIOO*, model ini memiliki beberapa tahapan yang harus diikuti oleh peneliti, antara lain: tahap persiapan berupa studi literatur, tahap perencanaan berupa pengumpulan kebutuhan, tahap desain berupa sekenario dan desain dari jaringan yang dibangun, tahap implementasi berupa konfigurasi, tahap *operate* berupa ujicoba, dan tahap optimasi berupa perbaikan.

Dengan metodologi ini akan memberikan langkah-langkah kunci untuk keberhasilan perancangan jaringan tersebut, dan peneliti melalui tahapan – tahapan dalam penelitian sesuai dengan model PPDIOO sebagai berikut:

1. *Prepare* (Persiapan)
   Dimana dalam tahapan ini penulis akan menyiapkan peralatan dan bahan-bahan atau studi literatur dengan cara mengumpulkan referensi yang ada dijurnal lima tahun terakhir agar memudahkan penulis dalam menjalankan penelitian. Adapun judul penelitian yang menjadi referensi antara lain:
   a. penelitian pada tahun 2018 dengan judul Analisis Perbandingan Performa Qos, PPTP, L2TP, SSTP dan IPSEC pada Jaringan VPN menggunakan Mikrotik (Zamalia, 2018).
   b. penelitian pada tahun 2016 mengenai Implementasi Remote Site pada *Virtual Private Network* Berbasis Mikrotik (Hendra, 2016).

c. penelitian pada tahun 2018 mengenai Implementasi *failover* pada Jaringan WAN Berbasis VPN (Siti, 2018).
d. Penelitian pada tahun 2019 mengenai Perancangan dan Implementasi *Virtual Private Network* (VPN) menggunakan Protocol SSTP Mikrotik di Fakultas MIPA Universitas Tanjungpura (Ikhwan, 2019).
e. Penelitian pada tahun 2016 mengenai Implementasi VPN *Server* dalam sistem Informasi Apotek (Masykuri, 2016).
f. Penelitian pada tahun 2019 dengan judul Penerapan metode PPDIOO pada jaringan internet Berbasis *WIRELESS (*Umam, 2019)

2. *Plan* (Perencanaan)
Pada Fase *Plan* (Perencanaan) yang merupakan tahap kedua dari PPDOO ini adalah penulis menganalisa kebutuhan kebutuhan *hardware* dan *software*, perancangan secara bertahap pekerjaan yang dilakukan serta bahan yang diperlukan.
Adapun dalam pengembangan sistem jaringan ini, spesifikasi kebutuhan perangkat keras dan perangkat lunak yang peneliti gunakan dalam penelitian ini, seperti pada tabel 1 dan 2 :

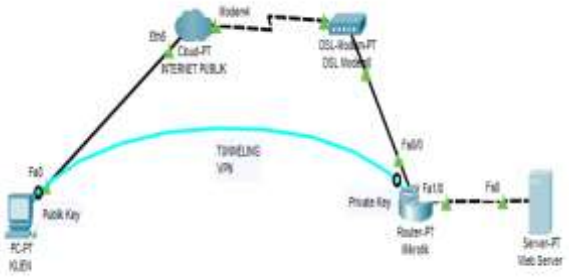
Tabel 1 Kebutuhan Perangkat Keras

No	Perangkat Keras	Spesifikasi
1	Laptop acer	Processor A8-4500M up to 2.80 GHz, GPU: AMD HD8750 2GB Vram, RAM 4GB, SSD 240GB, HDD 500GB
2	Mikrotik Routerboard	RB750GR3 HAX
3	Kabel UTP	CAT 5E

Tabel 2. Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Spesifikasi
1	Winbox	Versi 3.27
2	*Wireguard*	Versi 0.5.2
3	Google Chrome	Versi 80
4	Packet Tracer	Versi 7.3.0.xxx
5	Windows	Versi 8.1
6	Mikrotik RouterOS	Versi 7.1
7	Astah Profesional	Versi 8.2.0
8	Wireshark	Versi 3.2.6

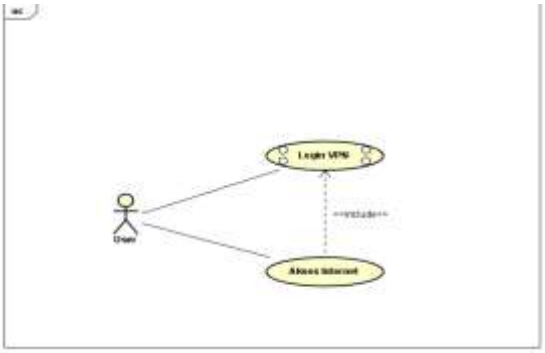
3. *Design* (Desain)
Setelah melakukan perencanaan, pada tahap selanjutnya yang dilakukan adalah mendesain topologi jaringan. Dimana pada tahapan ini penulis akan mendesain topologi jaringan dengan menggunakan *software packet tracer* versi 7.3.0 dan untuk diagram UML menggunakan *software astah professional*.



Gambar 1. Topologi Jaringan

Topologi yang dibuat pada tahapan desain akan digunakan sebagai acuan simulasi untuk tahapan selanjutnya. Sedangkan diagram UML yang dibuat antara lain: *use case diagram*, *activity diagram*, dan *deployment diagram*. Berikut ini diagram UML yang telah peneliti buat dari hasil analisa awal untuk menggambarkan interaksi *user* dan sistem jaringan yang akan digunakan.

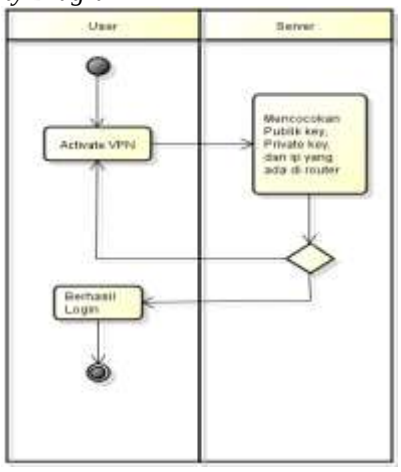
a. *Use Case*



Gambar 2. *Use Case*

Dari gambar 2, pengguna yang akan mengakses sistem menggunakan internet diharuskan untuk lebih dahulu mengaktifkan VPN agar komunikasi dapat di enkripsi, sehingga saat proses authentikasi berlangsung saat masuk ke sistem, komunikasi antar perangkat dapat lebih aman.

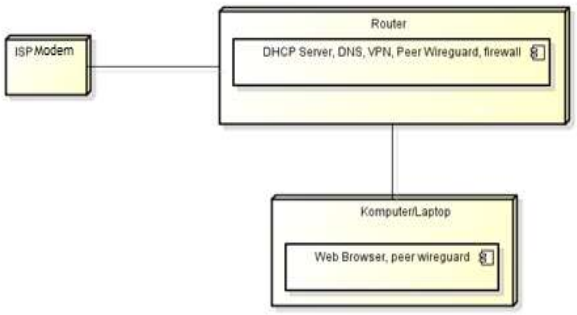
b. Activity Diagram



Gambar 3. *Activity Diagram*

Proses yang terjadi saat pengguna mengaktifkan VPN adalah proses pencocokan kunci kriptografi, baik yang publik maunpun private yang sudah didaftarkan pada masing – masing perangkat, apabila kunci nya sesuai maka VPN akan teraktifkan.

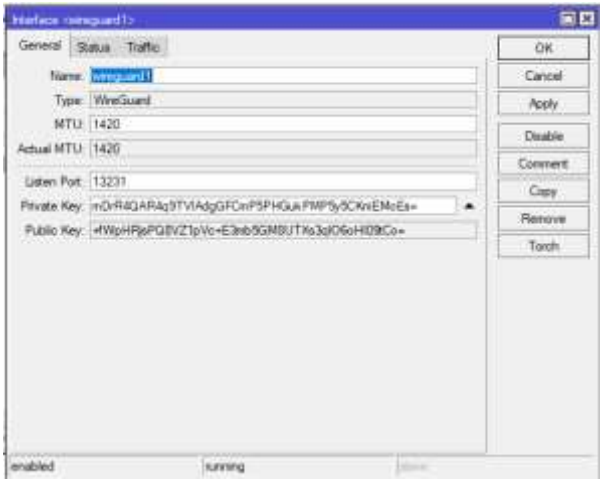
c. *Deployment diagram*



Gambar 4. *Deployment diagram*

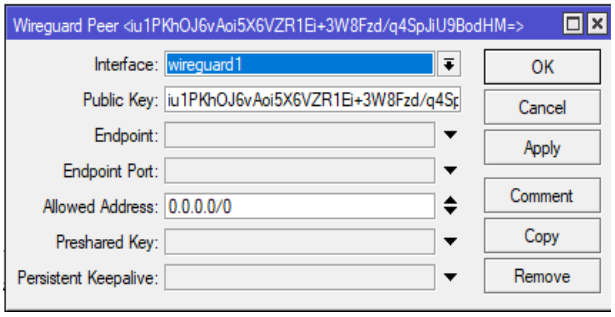
Terlihat pada gambar 4, untuk konfigurasi VPN nantinya akan sesuai dengan desain yang telah digambarkan oleh deployment diagram, dan dari gambar tersebut membutuhkan beberapa tool yang perlu dikonfigurasi baik dari router maupun perangkat yang digunakan oleh pengguna.

4. Implement (Implementasi)
Dalam tahap implement ini, penulis akan melakukan konfigurasi pada *wireguard* didalam mikrotik agar bisa terhubung dengan VPN dan dapat mengakses internet secara lancar dan aman.
Pengaturan awal dalam membuat *interface* VPN *wireguard* agar dapat mengakses internet, dilakukan dengan cara:
Buka menu *wireguard* >> add >> general >> name : *wireguard*1 >> apply dan ok, maka akan muncul *privatekey*, *publickey*, dan nilai aktual MTU secara otomatis. *Publickey* tersebut akan digunakan untuk menambah peer yang ada diperangkat peer *client*.



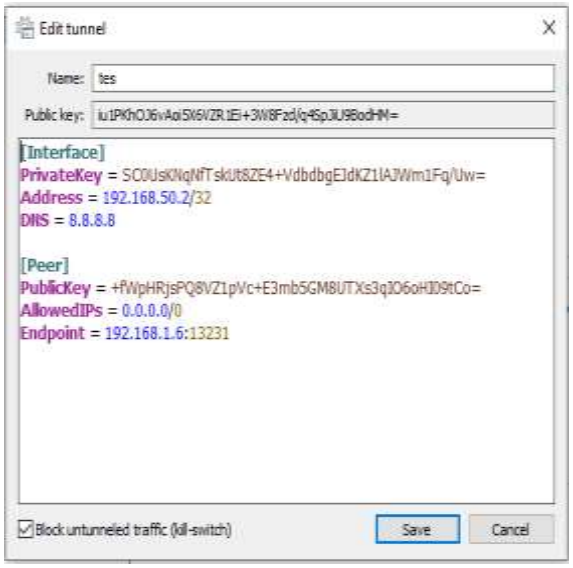
Gambar 5. Konfigurasi *Wireguard*

Langkah selanjutnya untuk menambah *wireguard* peer agar VPN bisa terhubung, dengan cara :
Klik menu *wireguard* >> peer >> add >> interface : *wireguard*1 >> public key : ambil dari aplikasi app *wireguard* >> Allowed addres : buat sendiri >> apply dan ok.



Gambar 6. Konfigurasi Peer *Wireguard*

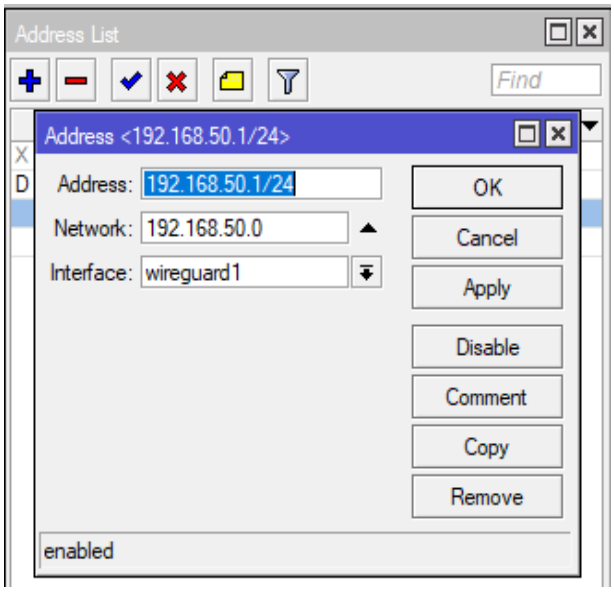
Setelah melakukan konfigurasi peer *wireguard* selanjutnya isi interface app *wireguard* dengan cara :
Buka aplikasi lalu Klik symbol segitiga yang ada disamping add tunnel >> pilih add empty tunnel >> Nama : tes >> edit address : ambil dari allowed address yang ada di *wireguard* peer mikrotik >> DNS : 8.8.8.8
Isi peer app *wireguard* >> public key : ambil dari interface *wireguard* yang ada di mikrotik dan salin >> AllowedIPs : 0.0.0.0/0 >> Endpoint : isi IP public >> angka ujung : ambil dari interface *wireguard* mikrotik >> listen port.



Gambar 7. Konfigurasi *tunnel Wireguard* klien

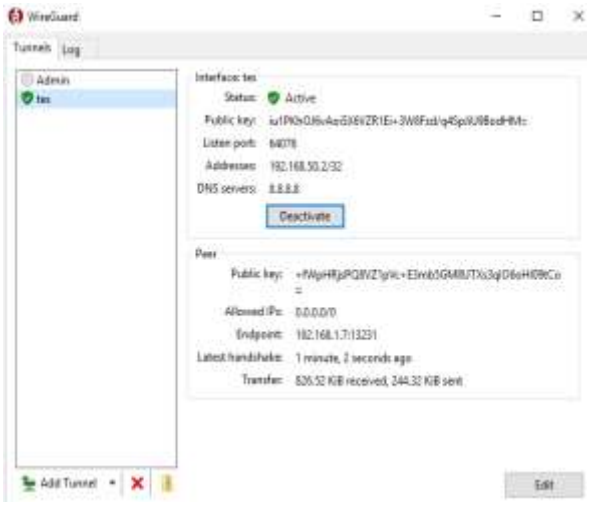
aplikasi *wireguard* tersebut di konfigurasi setelah di instal terlebih dahulu di perangkat klien yang akan digunakan sebagai peer *client*.
Selanjutnya buat IP *Wireguard* agar VPN bia terhubung dengan cara :
Buka IP >> address >> add >> address : 192.168.50.1/24 >> interface : *wireguard*1 >> apply dan ok.

VOLUME 13 Nomor 02 Agustus 2022
e-ISSN 2477-3786 | p-ISSN 2302-500X



Gambar 8. Konfigurasi Ip *Wireguard*

5. Operate (Mengoperasikan)
   Pada tahap *operate* akan dilakukan ujicoba jaringan dan dioperasikan secara langsung dengan melakukan konfigurasi yang sudah dirancang. Pada penelitian ini dilakukan uji coba untuk mengkoneksikan VPN *Wireguard* client dengan VPN *Wireguard* server untuk penghubungan jaringan apakah dapat terkoneksi atau tidak. Bila terjadi kekurangan atas sistem yang dibangun, dapat melakukan perbaikan sehingga sistem lebih optimal.
   Pada tahap ini dilalukan ujicoba untuk mengaktifkan VPN *Wireguard*, dengan menekan menu activate yang ada di app *wireguard* dan cek VPN sudah dapat terkoneksi atau belum.



Gambar 9. VPN yang sudah terkoneksi

6. Optimize (Optimasi)
   Pada tahap ini dilakukan dengan menganalisa kinerja jaringan yang sudah dibangun apakah telah berjalan dengan baik. Setelah dilakukan uji coba, tahap ini mengoptimalisasi terhadap sistem yang dibangun sesuai yang diharapkan.

2. Hasil dan Pembahasan

Pada tahap ini akan di tampilkan hasil dari penerapan sistem jaringan *wireguard* yang telah di buat sebelumnnya.

Selanjutnya penulis akan melakukan pengujian pada sistem untuk mengakses sistem di alamat http://spk.atmaluhur.ac.id tanpa VPN melalui jaringan publik, dimana alamat ip address dari perangkat klien seperti pada gambar 10.

Gambar 10. Alamat IP perangkat klien

Saat mengakses ke sistem menggunakan alamat ip tersebut, maka sistem akan menolak menampilkan data, dikarenakan alamat ip yang digunakan tidak masuk kedalam list ip yang diperbolehkan, dengan notifikasi seperti gambar 11.

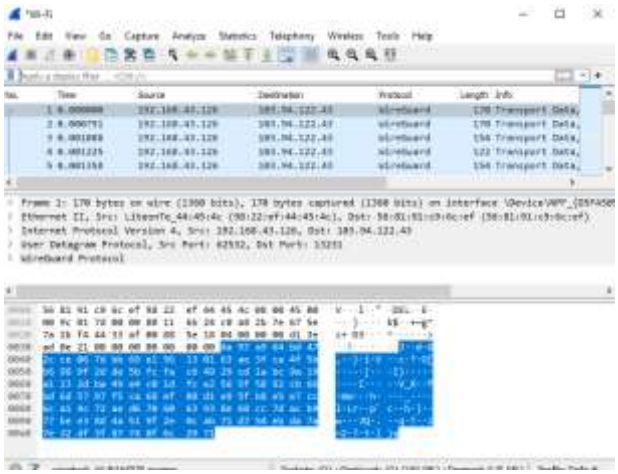
Gambar 11. Notifikasi alamat IP

Selanjutnya apabila VPN telah aktif, maka secara otomatis alamat ip dari perangkat pengguna akan berubah menjadi alamat ip yang terdaftar seperti gambar 12.

Gambar 12. Alamat IP terkoneksi VPN

Setelah alamat ip berubah, maka pengguna dapat terhubung ke sistem dan dapat mengakses seuluruh sumber daya sesuai dengan hak akses dari proses authentikasi sebelumnya, seperti yang terlihat pada gambar 13.

Gambar 13. Tampilan sistem yang diakses



Gambar 14. Tangkapan Data Komunikasi

Dari proses komunikasi antara perangkat klien dan server sistem, terlihat pada gambar 14 bahwa protokol yang digunakan adalah wireguard, dimana isi dari komunikasi tersebut meskipun mengkses sistem dengan protokol http yang tidak aman, akan isi komunikasinya tetap di enkripsi, sehingga kebocoran data dapat dihindari.

3. Kesimpulan

Setelah dilakukan penelitian ini, penulis dapat mengambil beberapa kesimpulan dari penulisan penelitian ini, sebagai berikut :

1. VPN *wireguard* ini mempunyai kelebihan yaitu mudah diimplementasikan dengan kemampuan melakukan enkripsi yang baik menggunakan kunci yang ada pada kedua peer, seperti terlihat pada hasil capture wireshark.
2. Aplikasi wireguard dapat berjalan dengan baik di sistem operasi windows 8.1 yang digunakan oleh klien.
3. Mekanisme kombinasi antara authentikasi dan VPN wireguard terbukti mampu menyembunyikan isi komunikasi di protokol http pada sistem.

Daftar Pustaka

Dian Novianto, Tri Sugihartono. 2020. Sistem Deteksi Kualitas Buah Jambu Air Berdasarkan Warna Kulit Menggunakan Algoritma Principal Component Analysis (Pca) dan K-Nearest Neigbor (K-NN). Jurnal Ilmiah Informatika Global Volume 11 No. 2 Desember 2020

Hendra Supendar. 2016. Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik. *Bina Insani ICT Journal*, *3*(1), 85-98.

http://mikrotik.co.id/artikel_lihat.php?id=407, diakses 20 oktober 2021.

Ikhwan Ruslianto. 2019. Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura. CESS (Journal of Computer Engineering, System and Science), 4(1), 74-77.

Imam Solikin. 2017. Penerapan Metode PPDIOO dalam Pengembangan LAN dan WLAN. Teknomatika, Vol.07, No.01, hal 65-73.

Irawan Afrianto , Eko Budi Setiawan. 2014. Kajian Virtual Private Network (Vpn) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom). Majalah Ilmiah Unikom Vol.12 No. 1.

Khasanah, S. N., & Utami, L. A. (2018). Implementasi Failover Pada Jaringan WAN Berbasis VPN. *Jurnal Teknik Informatika*, *4*(1), 62-66.

Masykuri, A., Utami, E., & Sudarmawan, S. (2016). Implementasi Vpn Server Dalam Sistem Informasi Apotek (Studi Kasus Integrasi Sistem Informasi Apotek Santi Pontianak). Data Manajemen dan Teknologi Informasi (DASI), 17(2), 7-12.

VOLUME 13 Nomor 02 Agustus 2022
e-ISSN 2477-3786 | p-ISSN 2302-500X

Umam, C. 2019. *Penerapan Metode Ppdioo Pada Jaringan Internet Berbasis Wireless (Studi Kasus: Kantor Desa Kabupaten Magelang)* (Skripsi, Universitas Muhammadiyah Magelang).

Zamalia, W. O., Aksara, L. F., & Yamin, M. (2018). Analisis PerbandinganPerforma Qos, Pptp, L2Tp, Sstp Dan IPsec Pada Jaringan Vpn Menggunakan Mikrotik. *semanTIK*, *4*(2), 29-36.