

IMPLEMENTASI VIRTUAL PRIVATE NETWORK MENGGUNAKAN POINT-TO-POINT TUNNELING PROTOCOL

Eka Satryawati¹⁾, Dwi Agung Pangestu²⁾, Ade Surya Budiman³⁾

¹⁾Prodi Sistem Informasi, Fakultas Komputer, Universitas MH Thamrin Jakarta

²⁾Prodi Teknik Informatika, FTI, Universitas Nusa Mandiri, Jakarta

³⁾Prodi Teknologi Komputer, FTI, Universitas Bina Sarana Informatika, Jakarta

Correspondence author: Eka Satryawati, ekathufail@gmail.com, Jakarta, Indonesia

Abstract

Today's technological development is very rapid, especially in the field of network security. The field of network security is a matter that will be a very important part because the network security system is used to guarantee the confidentiality, theft, or burglary of data on a company. In its implementation, a VPN network (Virtual Private Network) uses a site-to-site Point to Point Tunnel Protocol (PPTP) method to connect between two places that are located far apart. The main facility of using PPTP is being able to use a public-switched telephone network (PSTN) to build a VPN. At PT Indosis Integrasi Jakarta, the place where the author conducts research there are several problems that the author found, namely, when sending data between the head office and branch offices in Bandung, there is no security that ensures that the data is safe. With the current state of the network, uninterested parties will easily access or steal confidential company data.

Keywords: virtual private network, point-to-point tunneling protocol

Abstrak

Perkembangan teknologi dijamin sekarang sangat pesat, khususnya dibidang keamanan jaringan yang sangat mendasar bagi dunia teknologi internet. Dalam teknologi internet dibidang jaringan merupakan suatu hal yang akan menjadi bagian yang sangat penting, karena sistem keamanan jaringan digunakan untuk menjamin kerahasiaan, pencurian, ataupun pembobolan data pada suatu perusahaan. Dalam implementasinya, jaringan VPN (Virtual Private Network) menggunakan metode Point-To-Point Tunneling Protocol (PPTP) site-to-site untuk menghubungkan antara 2 tempat yang letaknya berjauhan. Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTN) untuk membangun VPN pada PT. Indosis Integrasi Jakarta, tempat dimana penulis melakukan riset terdapat beberapa permasalahan yang penulis dapati yaitu saat melakukan pengiriman data-data antara kantor pusat dan kantor cabang Bandung tidak adanya pengamanan yang memastikan bahwa data tersebut aman. Dengan keadaan jaringan saat ini, pihak-pihak yang tidak berkemungkinan akan mudah mengakses atau mencuri data perusahaan yang bersifat rahasia.

Kata Kunci: virtual private network, point-to-point tunneling protocol

A. PENDAHULUAN

Perkembangan teknologi sekarang ini sangat pesat, khususnya dibidang keamanan jaringan yang sangat mendasar bagi dunia teknologi internet. Dalam teknologi internet dibidang keamanan jaringan merupakan suatu hal yang akan menjadi bagian yang sangat penting, karena sistem keamanan jaringan digunakan untuk menjamin kerahasiaan, pencurian, ataupun pembobolan data pada suatu perusahaan.

Dengan semakin pesatnya teknologi, bukan berarti mengurangi permasalahan yang terjadi pada jaringan komputer. Seperti yang terjadi di PT. Indosis Integrasi, sering terjadi permasalahan keamanan jaringan komputer, ditambah dengan jarak yang cukup jauh antara kantor pusat dengan kantor cabang Bandung, sehingga menyebabkan kendala ketika ada permasalahan keamanan pada jaringan yang terjadi di kantor cabang Bandung tidak dapat diatasi dengan cepat.

Masalah seperti ini dapat terjadi bagi perusahaan yang memiliki kantor cabang yang letaknya berjauhan dengan kantor pusatnya. Untuk itu pihak perusahaan sangat mengharapkan adanya sistem jaringan komputer yang aman agar dapat digunakan untuk mengontrol, memonitoring dan mengatasi permasalahan keamanan jaringan di cabang Bandung secara cepat.

Menurut Prihatin Oktivasari dan Andri Budi Utomo, cara atau sistem yang dapat digunakan untuk melakukan hal tersebut adalah menggunakan Virtual Private Network (VPN). Dengan VPN sebuah instansi dapat memperlebar akses dengan aman terhadap jaringan internalnya melalui jaringan internet dengan biaya yang relatif lebih murah. Seluruh aplikasi dan data yang penting pada jaringan tersebut dapat diakses oleh pihak tertentu saja yang diberikan wewenang tanpa memperhatikan jarak dan tempat dimana diaksesnya (Oktivasari & Utomo, 2016).

Sebuah keamanan dalam berkomunikasi atau dalam pertukaran data, juga tidak memungkinkan pihak lain untuk menyusup ke *traffic* (lalu lintas jaringan) yang tidak semestinya. VPN adalah sebuah cara aman untuk mengakses *local area network* yang berada pada jangkauan, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi, dengan enkripsi perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya kedalam *remote-site* (Yuniati, Fitriawan, & Fahdi 2014). Sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antara jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur *privacy* dalam komunikasinya (Triyono, Rachmawati, & Irawan, 2014).

Dalam implementasinya, jaringan VPN (*Virtual Private Network*) menggunakan metode *Point-To-Point Tunneling Protocol* (PPTP) *site-to-site* untuk menghubungkan antara dua tempat yang berjauhan. *Point-To-Point Tunneling Protocol* (PPTP) merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access point-to-point protocol* (PPP) yang dikeluarkan *Internet Engineering Task Force* (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat dikirimkan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN to LAN dan komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN (Mufida, Irawan, & Chrisnawati, 2017). PPTP merupakan protokol jaringan yang

memungkinkan pengamanan transfer data remote klien ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Rachmawan & Prihanto, 2018). Point to Point Tunneling Protocol (PPTP) merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Putra, Indriyani, & Angraini, 2018).

Berdasarkan uraian permasalahan diatas maka penulis mengusulkan menggunakan metode PPTP pada jaringan VPN dimana ketika terjadi permasalahan jaringan pada kantor cabang Bandung dapat diremote dari kantor pusat dan dapat melakukan sharing file antara kantor pusat dan kantor cabang Bandung. Sehingga lalu lintas data yang dikirim dapat terjaga keamanan dan kerahasiaannya dari ancaman orang yang tidak bertanggung jawab.

B. METODE PENELITIAN

Teknik pengumpulan data yang digunakan oleh penulis adalah :

1. Observasi
Untuk mendapatkan hasil penelitian yang baik penulis melakukan pengamatan di PT. Indosis Integrasi Jakarta terhadap kondisi jaringan saat ini dan interkoneksi jaringan ke kantor cabang Bandung.
2. Wawancara
Dalam wawancara ini dilakukan tanya jawab dengan praktisi IT pada PT. Indosis Integrasi Jakarta, Administrator jaringan dan user yang ada di PT. Indosis Integrasi Jakarta dan beberapa orang yang ahli dalam jaringan.
3. Studi Pustaka
Untuk menelaah masalah secara mendalam dan untuk mencari solusi optimal terhadap permasalahan yang ada, maka penulis juga melakukan studi kepustakaan yaitu dengan mengumpulkan data – data teoritis dalam beberapa jurnal, artikel, dan mempelajari

buku – buku dengan maksud untuk mendapatkan teori – teori dan bahan – bahan yang berkaitan dengan masalah tersebut.

Analisa penelitian ini dilakukan sebagai salah satu alat proses untuk pengambilan keputusan, analisa penelitian ini berguna untuk mengurangi ketidakpastian dengan menyediakan informasi yang akurat untuk memperbaiki proses pembuatan keputusan itu. Tahapan penelitian yang penulis lakukan yaitu :

1. Analisa kebutuhan
Disini penulis juga pengumpulan data membutuhkan sebuah mikrotik yang dirancang agar saling terhubung antar mikrotik dengan menggunakan akses VPN dengan metode PPTP (Point-To-Point Tunnel protocol) dan untuk jaringan penulis menggunakan jaringan yang sudah berjalan di perusahaan PT. Indosis Integrasi Jakarta.
2. Desain
Penulis menggunakan sebuah mikrotik yang didesain membuat jaringan virtual atau simulasi menggunakan VMware sebagai penghubung agar koneksi antar cabang Bandung seakan - akan jaringan lokal.
3. Testing
Penulis melakukan testing dengan membuktikan koneksi jaringan antar cabang Bandung yang dirancang berjalan dengan maksimal.
4. Implementasi
Setelah membuat desain dan sudah melakukan testing berkali – kali sampai sebuah sistem rancang VPN menggunakan Point-to-Point tunnel protocol (PPTP) dengan mikrotik sudah berjalan dan berfungsi dengan maksimal, penulis baru bisa melakukan implementasi, agar pada saat sudah dijalankan tidak ada masalah.

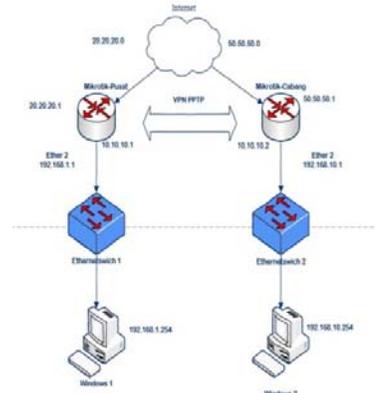
C. HASIL DAN PEMBAHASAN

Topologi Jaringan

Jaringan komputer pada PT.Indosis Integrasi Jakarta menggunakan star dimana pada topologi tersebut terdapat swith sebagai pusatnya. Server setiap komputer client dan piranti lainnya terhubung dengan menggunakan kabel.

Skema Jaringan

Pada skema jaringan, penulis tetap menggunakan skema jaringan yang sudah berjalan, karena skema jaringan yang sudah berjalan dirasa sudah sangat cukup baik hanya saja ditambahkan 1 buah PC Server untuk disetting menjadi Server VPN, baik dikantor pusat maupun dikantor cabang Bandung, dimana dimasing – masing PC tersebut nantinya bisa mengontrol PC lainnya yang ada pada jaringan di kantor cabang Bandung, sehingga jaringan kantor pusat dan cabang Bandung dapat saling terhubung secara aman menggunakan teknologi *Virtual Private Network (VPN)* dengan menggunakan metode *Point-to-Point Tunneling Protocol (PPTP)*.



Gambar 3. Skema Jaringan Usulan

Keamanan Jaringan

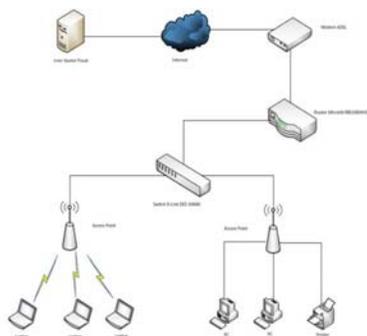
Menggunakan keamanan jaringan sangat diperlukan agar data serta informasi yang ada dapat terjaga dengan baik dan mencegah terjadinya upaya dari pihak lain seperti hacker. Selain dengan menggunakan metode PPTP (*Point-to-Point Tunneling Protocol*) setiap user yang hendak terhubung ke jaringan local masih harus verifikasi user dan password yang diminta oleh komputer server.

Rancangan Aplikasi

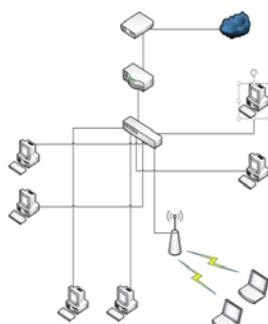
Konfigurasi yang akan digunakan yaitu dengan menerapkan metode PPTP (*Point-to-Point Tunneling Protocol*) yang akan dilakukan pada router mikrotik pada masing-masing kantor. Berikut ini adalah konfigurasi PPTP (*Point-to-Point Tunneling Protocol*) pada router mikrotik pusat yang berfungsi sebagai server VPN.

Konfigurasi PPTP

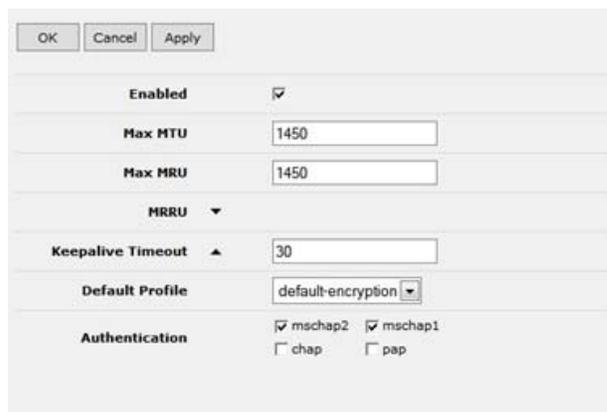
Untuk menggunakan fitur PPTP pada router mikrotik, beri tanda checklist pada enable terlebih dahulu untuk konfigurasi PPTP server pada mikrotik yang akan menjadi server PPTP, pada gambar dibawah adalah mikrotik dikantor pusat yang dipilih untuk menjadi server, masuk ke menu PPP pada menu bar mikrotik disebelah kiri lalu pilih PPTP server pada menu bar lalu checklist pada bagian enable.



Gambar 1. Skema Jaringan Kantor Pusat



Gambar 2. Skema jaringan Kantor Bandung



Gambar 4. Konfigurasi PPTP

Konfigurasi user PPTP

Pilih tab secret dimana tab ini berisikan konfigurasi pembuatan username dan password yang akan dapat mengakses jaringan local melalui internet. Pada kolom name isikan nama sesuai keinginan, pada gambar diatas disii dengan nama “server” dan pada password diisi “1234567890”.

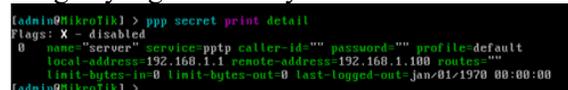
Lalu pada kolom local address diisi dengan IP public atau IP address router mikrotik yang berada dikantor pusat atau yang menjadi server pada kolom remote address diisi dengan alamat IP address yang nantinya akan diberikan pada user apabila sudah berhasil mengakses PPTP server pada router mikrotik yang berada dikantor pusat sudah selesai dibuat, untuk mengakses PPTP VPN tersebut dapat dilakukan pada mikrotik cabang Bandung.



Gambar 5. Konfigurasi user PPTP

Konfigurasi VPN client

Pada bagian connectto diisikan IP address pusat sedangkan untuk kolom username dan password isikan sesuai dengan username dan password sesuai dengan yang sebelumnya sudah dibuat.



Gambar 6. Konfigurasi VPN client

Manajemen Jaringan

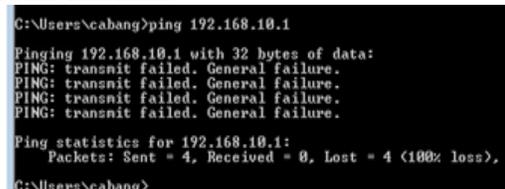
Sangat penting untuk melakukan manajemen jaringan dalam membangun suatu jaringan komputer apalagi jika jaringan sudah sangat luas cakupannya. Agar proses berbagi data lebih terjamin keamanannya dan menjaga jaringan tetap berjalan dengan baik.

Pada penerapannya metode *tunneling protocol* ini sangat membantu administrator jaringan untuk lebih mudah mengawasi, memonitoring jaringan komputer yang sedang berjalan dan pengambilan data tanpa harus melakukan kunjungan ke kantor cabang.

Pengujian Jaringan Awal

Pada tahap pengujian awal dilakukan sebelum adanya penerapan metode tunneling PPTP pada router mikrotik dapat dilihat bahwa setiap user pada masing – masing kantor belum dapat terhubung.

Penulis melakukan test ping pada user yang berada dikantor pusat ke user yang berada dikantor cabang Bandung, dapat dilihat bahwa transmits failed. General failure atau bisa juga disebut system tidak bisa mengirimkan paket ping antara kantor pusat dengan kantor cabang Bandung karena suatu masalah.



Gambar 7. Test Ping pusat – cabang Bandung kondisi awal

Dari gambar dibawah dapat dilihat bahwa hasil ping juga menunjukkan hasil yang sama dengan percobaan sebelumnya. Hal ini terjadi karena belum terhubungnya kantor cabang Bandung dengan kantor pusat.

```
C:\Users\cabang>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
PING: transmit failed. General failure.
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\cabang>
```

Gambar 8. Test Ping cabang Bandung – pusat kondisi awal

Pengujian Jaringan Akhir

1. Test Ping

Dalam percobaan ini penulis melukan test ping pada user yang berada dikantor pusat ke user kantor cabang,Bandung dapat dilihat bahwa sudah terjalin komunikasi atau jaringan sudah terkoneksi.

```
C:\Users\cabang>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=6ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
C:\Users\cabang>
```

Gambar 9. Test Ping pusat – cabang Bandung (Setelah pengujian)

Penulis juga melakukan percobaan yang sama pada user kantor cabang Bandung test ping dengan user yang berada kantor pusat, dapat dilihat bahwa permintaan sudah direspon atau jaringan sudah terkoneksi antar kantor cabang Bandung dengan kantor pusat.

```
C:\Users\cabang>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\cabang>
```

Gambar 10. Ping cabang Bandung – pusat (setelah pengujian)

2. Test Traceroute

Kemudian untuk pengetesan traceroute penulis juga melakukan pengentesan “Traceroute” sebelumnya yaitu tiap kantor dan juga melalui jaringan VPN yang sudah terbentuk.

Gambar dibawah adalah pengetestan trace route dari kantor pusat ke ykantor cabang Bandung dimana dapat dilihat yaitu bahwa rute paket yang dilewati yaitu melauai 192.168.1.1 yaitu gateway LAN kantor pusat dan gateway PPTP tunneling kantor cabang yaitu 192.168.10.1.

```
C:\Users\cabang>tracert 192.168.1.1
Tracing route to 192.168.1.1 over a maximum of 30 hops
  0  <1 ms  <1 ms  <1 ms  192.168.1.1
Trace complete.
C:\Users\cabang>
```

Gambar 11. Traceoute pusat ke cabang Bandung (setelah pengujian)

Gambar dibawah adalah pengetestan trace route dari kantor cabang ke kantor pusat dimana dapat dilihat yaitu bahwa rute paket yang dilewati yaitu melalui 192.168.10.1 yaitu gatewayLAN kantor cabang Bandung dan gateway PPTP tunneling kantor cabang Bandung yaitu 192.168.1.1.

```
C:\Users\cabang>tracert 192.168.1.1
Tracing route to 192.168.1.1 over a maximum of 30 hops
  0  <1 ms  <1 ms  <1 ms  192.168.1.1
Trace complete.
C:\Users\cabang>
```

Gambar 12. Traceroute cabang Bandung ke pusat (setelah pengujian)

D. PENUTUP

VPN adalah sebuah koneksi Virtual yang bersifat private, disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut private karena jaringan ini merupakan jaringan yang sifatnya private dan tidak semua orang bisa mengaksesnya.

VPN dapat mengirim data antara dua komputer yang melewati jaringan publik

sehingga seolah – olah terhubung secara Point-To-Point.

Data yang dikirimkan dienkapsulasi dan di enkripsi kedalam bentuk pecahan data dengan header yang berisi informasi routing untuk mendapatkan koneksi Point-To-Point sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan.

Point-To-Point Tunneling Protocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server perusahaan dengan suatu Virtual Private Network (VPN) melalui jaringan data berbasis TCP/IP.

Untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang ditangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut “Tunneling”.

Dengan menggunakan VPN PPTP dapat mengurangi biaya operasional bila dibandingkan dengan menggunakan aplikasi Hamachi untuk mengirim file secara rahasia dan aman.

E. DAFTAR PUSTAKA

- Amillia, F., Marzuki, & Agustina. (2014). Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) dan Geographic Routing Protocol (GRP) Pada Mobile Ad Hoc Network. *Manet*. 12(1), 9–15.
- Khasanah, S. N., & Kuryanti, S. J. (2019). Rancangan Virtualisasi Server Menggunakan VMWare Vsphere. *EVOLUSI - Jurnal Sains Dan Manajemen*, 7(1), 42–46. <https://doi.org/10.31294/evolusi.v7i1.5091>
- Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site Mikrotik VPN dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta.
- Muftikhali, Q. E., Yansen, A., Danar, F., Kusumawati, A., & Hidayat, S. (2018). Optimasi Algoritma Genetika Dalam Menentukan Rute Optimal Topologi Cincin Pada Wide Area Network. 13(1), 1–6.
- Oktivasari, P., & Utomo, A. B. (2016). Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol Analysis of Virtual Private Network Using Openvpn and Point To. *Jurnal Penelitian Komunikasi Dan Opini Publik*, 20(2), 185–202.
- Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. *Asri Pancawarna*. 3(2), 260–267.
- Rachmawan, A., & Prihanto, A. (2018). Jurnal Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet Di atas VPN. 53–57.
- Triyono, J., Rachmawati, Y., & Irnawan, F. D. (2014). Analisa Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data. 1(2), 112–121.
- Varianto, E., & Badrul, M. (2015). Implementasi Virtual Private Network dan Proxy Server Menggunakan Clear OS Pada PT. *Valdo Internasional*. 1(1), 54–65.
- Yuniati, Y., Fitriawan, H., Fahdi, D., & Patih, J. (2014). Analisa Perancangan Server VOIP (Voice Internet Protocol) Dengan OpenSource Asteriks dan VPN (Virtual Private Network). 12(1), 112–121.