

## RANCANG BANGUN JARINGAN SITE TO SITE VPN (VIRTUAL PRIVATE NETWORK) DENGAN PROTOCOL OPENVPN

**Usanto S.**

Prodi Sistem Informasi, Fakultas Teknologi, ITB Swadharma Jakarta

Correspondence author: Usanto S, [usanto.s@swadharma.ac.id](mailto:usanto.s@swadharma.ac.id), Jakarta, Indonesia

### **Abstract**

The use of wireless media such as the internet in building computer networks is so widely used. However, performance and security must also be considered. VPN (Virtual Private Network) is one of the methods in network security that works by creating a tunnel so that a trusted network can connect to networks outside via the internet. PT. Laris Manis Utama is a private company engaged in the field of fresh fruits export-import and distributor. And already has several branch offices located outside the city. Designing a VPN (Virtual Private Network) with a Site to site (OpenVPN) system at PT. Laris Manis Utama functions as a communication liaison for media and data transfer between the head office server and branch servers so that they are connected in real-time and can develop application systems and updated databases.

**Keywords:** *network, site-to-site VPN, OpenVPN*

### **Abstrak**

Penggunaan media tanpa kabel seperti internet dalam membangun jaringan komputer banyak digunakan. Akan tetapi, faktor kinerja dan keamanan harus juga diperhatikan. VPN (*Virtual Private Network*) adalah salah satu metode dalam pengamanan jaringan yang bekerja dengan cara membuat suatu *tunnel* sehingga jaringan yang dipercaya dapat terhubung dengan jaringan yang ada di luar melalui internet. PT. Laris Manis Utama merupakan perusahaan swasta yang bergerak di bidang *fresh fruits export – import and distributor*. Telah memiliki beberapa kantor cabang yang berada di luar kota. Perancangan VPN (*Virtual Private Network*) dengan sistem *Site to site (OpenVPN)* di PT. Laris Manis Utama berfungsi sebagai media penghubung komunikasi maupun transfer data antara server kantor pusat dengan server kantor cabang agar terkoneksi secara *realtime* dan dapat melakukan pengembangan sistem aplikasi maupun *database* secara *update*.

**Kata Kunci:** *jaringan, internet, VPN, OpenVPN*

## A. PENDAHULUAN

Pada era globalisasi sekarang ini, manfaat dari jaringan komputer sudah sangat banyak dirasakan. Apalagi dalam dunia komunikasi yang serba cepat ini, jaringan komputer sering kali berperan vital dalam kegiatan pendistribusian informasi yang cepat. Jaringan komputer merupakan suatu himpunan interkoneksi sejumlah komputer, dan merupakan kumpulan beberapa komputer, dan perangkat lain seperti router, switch dan sebagainya, (Sofana, 2013:3). Jaringan komputer pertama di rancang dengan perangkat keras yang menjadi pertimbangan utamanya, dan perangkat lunak menjadi pertimbangan selanjutnya, (Sugeng, 2015:11).

Semua dari komponen yang tergabung dalam jaringan komputer tersebut haruslah mampu saling mendukung untuk menghasilkan suatu sistem yang efisien untuk melayani setiap permintaan informasi yang dibutuhkan oleh pengguna.

Oleh itu ketersediaan jaringan komputer saat ini sangatlah penting untuk menunjang komunikasi bahkan untuk menunjang pekerjaan kita selama 24 jam setiap harinya. Jaringan komputer merupakan kumpulan komputer, printer dan peralatan lainnya yang terhubung antara satu dengan yang lain, (Silitonga & Morina, 2014:19).

Jaringan komputer adalah kumpulan sekelompok komputer yang semuanya saling berhubungan dengan menggunakan media perantara, sehingga antar komputer tersebut dapat saling terhubung dan berkomunikasi. Adapun media perantara untuk membangun jaringan komputer ini berupa media kabel ataupun media tanpa kabel (nirkabel).

Penggunaan media tanpa kabel seperti internet dalam membangun jaringan komputer begitu banyak digunakan. Akan tetapi, hal kinerja dan keamanan harus diperhatikan dalam hal ini. VPN (Virtual Private Network) adalah salah satu metode dalam pengamanan jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang dipercaya dapat

menghubungkan jaringan yang ada di luar melalui internet. VPN (virtual private network), yaitu 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 walaupun menggunakan medium yang umum, tetapi lalu lintas (traffic) antar remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidak semestinya ke dalam remote-site, (Ical, 2011)

VPN (Virtual Private Network) merupakan sebuah jaringan private yang menghubungkan satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan public (open connection/virtual circuit) seperti internet guna menghubungkan beberapa jaringan lokal, (Sofana, 2012:228) seperti Internet. VPN merupakan sebuah sarana untuk mengamankan dan memprivatkan pengiriman data melalui sebuah infrastruktur jaringan yang tidak aman dan dapat digunakan bersama (shared), Sedangkan untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut "tunneling". Dan dikelompokkan menjadi 5 yaitu : (1). User Authentication (VPN harus mampu mengklarifikasi identitas klien serta membatasi hak akses user sesuai dengan otoritasnya), (2) Address Management (VPN harus dapat mencantumkan address klien pada intranet dan memastikan alamat/address tersebut tetap rahasia), (3) Data Encryption (Data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak atau klien yang tidak berwenang), (4) Key Management (VPN harus mampu membuat dan memperbarui encryption key untuk server dan

klien), dan (5) Multiprotocol Support (VPN harus mampu menangani berbagai macam protokol dalam jaringan publik seperti IP, IPX dan sebagainya), (Wendy and Ramadhana 2008).

Protokol Tunneling VPN terbagi menjadi 4 yaitu (1) Tunneling merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi point-to-point dari sumber ketujuannya. Disebut tunnel karena koneksi point-to-point tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket – paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP Addressing dan IP Routing yang sudah baik atau telah terhubung sehingga antara sumber tunnel dengan tujuan tunnel dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari tunnel tidak dapat berjalan dengan baik, maka tunnel tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun. (2) Point to Point Tunneling Protocol (PPTP), dikembangkan oleh Microsoft dan Cisco 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 yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui internet, PPTP juga dapat digunakan pada jaringan private LAN-to-LAN, (3) Layer 2 Tunneling Protocol (L2TP), adalah tunneling protocol yang memadukan dua buah tunneling protocol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua

jenis protokol komunikasi didalamnya, (Gupta 2007). Umumnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP encapsulated PPP frames sebagai data yang di tunnel. Terdapat dua model tunnel yang dikenal, yaitu compulsory dan voluntary. (4) IP Security (IPSec), merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan layer yang berada di atasnya. IPSec (Internet Protocol Security) merupakan salah satu mekanisme yang diimplementasikan pada Virtual Private Network. Paket IP tidak memiliki aspek security, maka hal ini akan memudahkan untuk mengetahui isi dari paket dan alamat IP itu sendiri.

Salah satu perusahaan yang telah menggunakan jaringan komputer antara lain PT. Laris Manis Utama. Jaringan komputer disini dapat dikatakan cukup besar, sebagai perusahaan yang bergerak di bidang fresh fruits export – import and distributor, kegiatan seperti pertukaran dan pengiriman data sangat di butuhkan. Jaringan komputer di PT. Laris Manis Utama tidak hanya dipakai pada jaringan lokal saja tetapi juga dapat digunakan untuk akses internet. PT. Laris Manis Utama saat ini telah memiliki delapan kantor cabang yang berada di luar kota, namun memiliki kendala disebabkan karena tidak adanya media yang terkoneksi secara realtime, sehingga tidak dapat melakukan pengembangan sistem aplikasi database secara update, sesuai dengan periode waktu yang bersamaan dan berkala antara server kantor pusat dengan server cabang, dikarenakan proses komunikasi data yang berjalan saat ini hanya menggunakan email. Penyediaan server jaringan secara terpisah sudah menjadi kebutuhan tersendiri, terutama di kalangan institusi pendidikan atau perusahaan yang memiliki komputer klien dalam jumlah banyak, (Kurniawan, 2014:97)

Berdasarkan permasalahan tersebut, maka PT. Laris Manis Utama memerlukan suatu sistem jaringan VPN (Virtual Private Network) dengan sistem site to site (openvpn)

secara private di dalam jaringan publik dengan koneksi yang ekonomis dan keamanan data yang terjamin. Berfungsi sebagai media penghubung komunikasi maupun transfer data antara server kantor pusat dengan server cabang agar terkoneksi secara realtime dan dapat melakukan pengembangan sistem aplikasi maupun database secara update.

Penelitian ini bertujuan untuk merancang sistem jaringan Virtual Private Network PT. Laris Manis Utama sebagai media penghubung antara server pusat dengan server cabang agar dapat terkoneksi secara real time, dan dengan mengimplementasikan jaringan Virtual Private Network di PT. Laris Manis Utama untuk memperbaiki sistem jaringan komunikasi data dan mengimplementasikan pengembangan sistem aplikasi maupun database secara update.

## B. METODE PENELITIAN

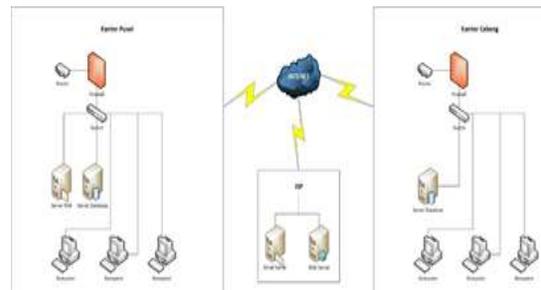
Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Penelitian ini menggunakan metode penelitian kualitatif dengan menggunakan pendekatan penelitian pengamatan (observasi) merupakan suatu proses yang kompleks, suatu proses yang tersusun dari berbagai proses biologis dan psikologis, (Sugiyono, 2017:145).

1. Teknik Observasi yaitu melakukan penelitian secara langsung ke lapangan untuk mengadakan pengamatan terhadap kegiatan proses komunikasi data di PT. Laris Manis Utama.
2. Teknik Wawancara digunakan sebagai teknik pengumpulan data dengan melakukan tanya jawab langsung dengan para staff dan Manager Operasional.
3. Studi Pustaka langkah-langkah ilmiah dalam mengumpulkan data dengan mencari referensi pendukung, (Chaidir & Rino, 2019:252). Studi pustaka dilakukan dengan mencari referensi jurnal-jurnal dan buku-buku yang terkait. Untuk

pengumpulan data sekunder dilakukan untuk memperoleh keterangan dan data dari literatur yang berupa buku, majalah, makalah, internet yang relevan dengan landasan teori atas masalah yang diteliti agar diperoleh suatu pemahaman yang mendalam serta menunjang proses pembahasan mengenai masalah-masalah yang telah diidentifikasi.

## C. HASIL DAN PEMBAHASAN

Sistem jaringan komputer di PT. Laris Manis Utama bersifat terpusat baik sistem jaringan data maupun komunikasi serta berbagi sumber ke semua kantor cabang melalui media internet. Untuk kebutuhan jaringan internet PT. Laris Manis Utama menggunakan perusahaan penyelenggara jasa koneksi internet (ISP) guna menyediakan layanan komunikasi data melalui media internet agar PT. Laris Manis Utama mempunyai area jaringan lokal yang besar sehingga bisa terhubung dengan kantor cabang. Sistem jaringan PT. Laris Manis Utama yang selama ini di jalankan dapat dilihat pada gambar 1



Gambar 1 Sistem Jaringan Berjalan

Tabel 1. Sistem Koneksi Internet ISP

Kantor pusat	
Perusahaan ISP	PT. Telkom
Jenis Koneksi	Speedy ADSL
Bandwidth	30 Mbps
IP Publik	Static

Kantor cabang	
Perusahaan ISP	PT. Telkom
Jenis Koneksi	Speedy ADSL
Bandwidth	10 Mbps
IP Publik	Dynamic

Dalam menganalisa sistem jaringan komputer di PT. Laris Manis Utama menggunakan suatu metode PIECES (*Performance, Information, Economics, Control, Efficiency, Service*).

1. *Performance*, sistem jaringan yang berjalan saat ini masih belum efisien, dikarenakan sistem jaringan server pusat dengan cabang masih belum terkoneksi secara realtime sehingga tidak dapat melakukan update database maupun software atau aplikasi lainnya secara berkala dan bersamaan.
2. *Information*, sering terjadi keterlambatan informasi pengiriman data dalam pelaksanaan proses kegiatan operasional pada saat pengolahan data perusahaan dan karyawan.
3. *Economics*, belum terintegrasinya komunikasi data antara server pusat dengan cabang mengakibatkan proses pengolahan data pengiriman barang membutuhkan waktu yang lebih lama sehingga kurang ekonomis.
4. *Control*, pemantauan dan pemeliharaan terhadap sistem jaringan yang saat ini berjalan masih kurang maksimal. Dikarenakan terbatasnya area jangkauan jaringan yang masih belum terhubung antara server pusat dengan cabang.
5. *Efficiency*, pengaruh dari belum terintegrasinya sistem jaringan antara server pusat dan cabang mengakibatkan komunikasi data dan pengelolaannya menjadi kurang efisien.
6. *Service*, sistem jaringan yang berjalan saat ini belum dapat menunjang proses komunikasi dan pengelolaan data pengiriman barang dengan baik sehingga secara keseluruhan pelayanan proses

pengiriman barang menjadi terganggu dan terhambat.

Berdasarkan analisa PIECES diperoleh salah satu solusi yang diberikan untuk menghadapi masalah jaringan pada PT. Laris Manis Utama adalah dengan menggunakan teknologi VPN. VPN bekerja membentuk suatu pipa (tunnel) yang berada didalam jaringan publik sehingga aliran data yang lewat didalamnya tidak bisa diakses oleh orang yang tidak memiliki hak akses ke dalam tunnel tersebut. Sehingga nantinya data – data yang dikirim oleh PT. Laris Manis Utama antara kantor pusat dengan kantor cabangnya yang lebih banyak bersifat rahasia dapat terjaga keamanannya dan juga lebih efisien dalam hal pengiriman data. Pada bab ini akan dijelaskan langkah – langkah dalam merancang suatu VPN, mulai dari menentukan tipe VPN yang akan digunakan, topologi VPN yang akan digunakan dan teknologi VPN yang akan digunakan. Berdasarkan lokasi dan informasi yang dipertukarkan maka tipe VPN yang cocok adalah tipe *Site-to-Site Intranet VPN* dengan *Site-to-Site Intranet VPN*, jaringan kantor pusat dan cabang terhubung menjadi satu jaringan internal tersendiri.

Sesuai dengan proses bisnis yang telah dijelaskan sebelumnya bahwa sering terjadinya proses pertukaran data yang dilakukan antara kantor pusat dan kantor cabang di tiap bagian. Dengan terhubungnya kantor pusat dan kantor cabang dengan VPN ini memudahkan proses pertukaran data menjadi selalu terupdate sehingga proses bisnis yang berjalan dikantor pusat dan kantor cabang dapat berjalan menjadi lebih efisien. Selain itu topologi ini juga mudah untuk dikembangkan bila perusahaan ini berniat membuka cabang baru dan menghubungkannya dengan jaringan kantor pusat

*OpenVPN* merupakan aplikasi *open source* untuk *Virtual Private Network (VPN)*, dimana aplikasi tersebut dapat membuat koneksi *point-to-point tunnel* yang telah terenkripsi. Dimana teknologi yang

digunakan untuk enkripsi, dalam jaringan *OpenVPN* ini menggunakan teknologi SSL dan untuk komunikasinya *OpenVPN* bergerak di Layer 2 dan Layer 3 OSI Layer. Karena *OpenVPN* berbasis *protocol* SSL maka *OpenVPN* ini dapat digunakan di berbagai sistem operasi tanpa perbedaan yang signifikan. *Tunnel* yang dibangun antar *network* didapatkan melalui satu *port* TCP atau port UDP dan menggunakan semua fitur *Open* SSL untuk otentikasi, sertifikasi, enkripsi untuk menjaga keutuhan dan keamanan data yang dilewatkan jaringan publik.

Tiap divisi memiliki kebutuhan yang sama terhadap jaringan komputer, selain untuk mengakses *resource* pada komputer lain, seperti file atau printer, jaringan komputer juga dimanfaatkan untuk mengakses server database yang menyimpan data proses bisnis perusahaan.

Adapun IP Address yang akan digunakan untuk perancangan jaringan yang diusulkan untuk kantor pusat dapat dilihat pada tabel 2

Tabel 2. IP Address Jaringan Kantor Pusat

NO	SERVER	ALAMAT IP	KET
1	ClearOS Pusat	92.168.10.10/24	IP Address
		255.255.255.0	Subnet
		192.168.10.0	Network
	DIVISI	ALAMAT IP	SUBNET
2	Direktu	192.168.10.11	255.255.255.0
3	Wakil Direktur	192.168.10.12	255.255.255.0
4	Internal Audit	192.168.10.13-16	255.255.255.0
5	Corporate HRD & Legal	192.168.10.17	255.255.255.0
6	Corporate Accounting	192.168.10.18	255.255.255.0
7	Corporate Finance	192.168.10.19	255.255.255.0
8	Corporate Operasional	192.168.10.20	255.255.255.0
9	HRD	192.168.10.21-24	255.255.255.0
10	Legal	192.168.10.25	255.255.255.0
11	Pajak	192.168.10.26-36	255.255.255.0
12	Accounting	192.168.10.37-46	255.255.255.0
13	Finance	192.168.10.47-59	255.255.255.0
14	Import	192.168.10.60-69	255.255.255.0
15	Admin Gudang	192.168.10.70-75	255.255.255.0
16	General Affair	192.168.10.76-78	255.255.255.0
17	IT	192.168.10.79-82	255.255.255.0
18	Operasional	192.168.10.83-88	255.255.255.0

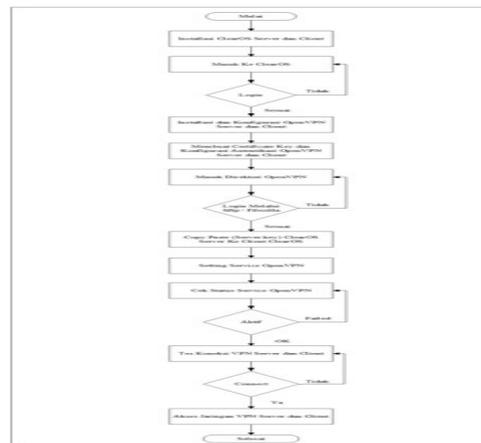
19	Admin Marketing	192.168.10.89-94	255.255.255.0
20	Marketing	192.168.10.95-110	255.255.255.0
21	Kas Kecil	192.168.10.111-113	255.255.255.0
22	Pool / Kendaraan	192.168.10.114-116	255.255.255.0

Selain kantor pusat, PT. Laris Manis Utama juga memiliki kantor cabang pemasaran yang berada di luar kota. Berikut ini adalah rancangan pengalamanan IP pada kantor cabang dan dapat dilihat pada tabel 3

Tabel 3. IP Address Jaringan Kantor Cabang

NO	SERVER	ALAMAT IP	KET
1	ClearOS Pusat	192.168.20.10/24	IP Address
		255.255.255.0	Subnet
		192.168.20.0	Network
	DIVISI	ALAMAT IP	SUBNET
2	Kepala Cabang	192.168.20.11	255.255.255.0
3	HRD	192.168.20.12-13	255.255.255.0
4	Pajak	192.168.20.14	255.255.255.0
5	Accounting	192.168.20.15-17	255.255.255.0
6	Finance	192.168.20.18-20	255.255.255.0
7	Import	192.168.20.21-25	255.255.255.0
8	Admin Gudang	192.168.20.26-27	255.255.255.0
9	IT	192.168.20.28-29	255.255.255.0
10	Admin Marketing	192.168.20.30-33	255.255.255.0
11	Marketing	192.168.20.34-38	255.255.255.0
12	Kas Kecil	192.168.20.39	255.255.255.0
13	Pool / Kendaraan	192.168.20.40	255.255.255.0

Flowchart Rancangan Virtual Private Network (VPN) dapat dilihat pada gambar 2

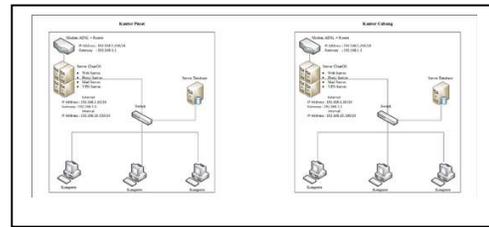
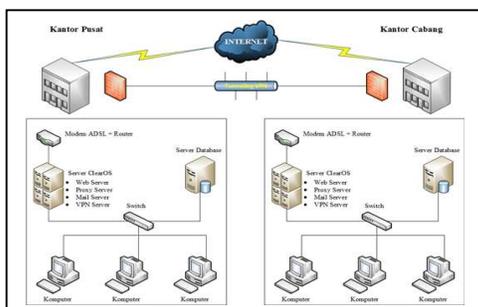


Gambar 2. Flowchart Rancangan VPN

*Topologi* jaringan LAN yang digunakan adalah *topologi star* karena pada *topologi* ini setiap *workstation* dikoneksikan pada satu perangkat central, perangkat ini berfungsi untuk mengatur komunikasi data pada setiap workstation. Sehingga mudah dalam mendeteksi *error*, dan jika salah satu *workstation* rusak maka perangkat yang rusak tidak mengganggu *workstation* lain. *Topologi* star merupakan *topologi* yang setiap perangkatnya di hubungkan pada satu perangkat penghubung (sentral) keperangkat-perangkat yang lain, (Nugroho, 2016:11)

Pada masing – masing kantor pusat dan kantor cabang dipasang sebuah perangkat PC Server dengan *Operating System ClearOS* dengan sistem mode gateway, perangkat ini bertindak sebagai *embedded gateway* dari masing – masing site. Setiap aliran data yang dikirim dari kantor cabang ke kantor pusat atau sebaliknya akan melewati *gateway* tersebut. Sebelum melalui proses pengiriman data antar kantor pusat dan kantor cabang tersebut, agar data yang dikirimkan menjadi lebih aman, data tersebut akan dikapsulasi terlebih dahulu dan baru kemudian akan didekapsulasi diujung *gateway* lainnya setelah proses pengiriman tersebut, sehingga data – data tersebut tidak mudah dibaca oleh orang lain. Koneksi internet yang akan digunakan pada kantor pusat untuk mendukung VPN menggunakan dedicated internet 30 Mbps dan IP Statics sedangkan koneksi pada kantor cabang dedicated internet 10 Mbps. Kantor cabang dan pusat menggunakan provider ISP Telkom.

Rancangan koneksi Jaringan kantor pusat dan kantor cabar dengan VPN pada PT. Laris Manis Utama dapat dilihat pada gambar 3



Gambar 3. Jaringan VPN PT. Laris Manis Utama

### Rancangan Implementasi Jaringan VPN

Untuk implementasi dan perancangan jaringan VPN, maka dibutuhkan analisis beberapa perangkat lunak dan perangkat keras yang akan digunakan untuk dapat memenuhi kebutuhan dan mencapai tujuan yang diinginkan dapat dilihat pada tabel 4 dan 5

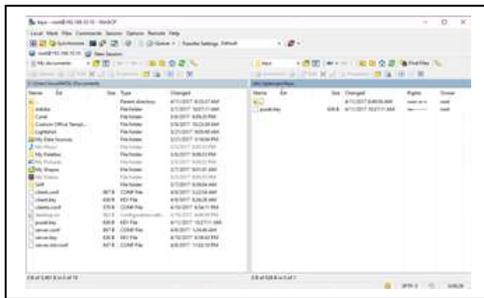
Tabel 4. Spesifikasi Server Kantor Pusat

No	Per. Keras	Unit	Keterangan
1	PC server	1	➤ Processor : Xeon 3,5 Ghz ➤ RAM : 8 GB ➤ Harddisk : 350 GB
2	Router	1	➤ TP-LINK TD-W8968 ADSL2 + MODEM /300mbps
3	Kabel UTP	1	➤ Cat 5e
4	LAN CARD	2	➤ TP-LINK 100/mbps
5.	Switch	1	➤ HP Procurve 2510-24 J9019B
No	Per. Lunak	Unit	Keterangan
1	Sistem Operasi (OS)	1	➤ ClearOS 5.2
2	OpenVpn	1	➤ OpenVpn rc2.1

Tabel 5. Spesifikasi Server Kantor Cabang

No	Per. Keras	Unit	Keterangan
1	PC server	1	➤ Processor :Xeon3,5 Ghz ➤ RAM : 8 GB ➤ Harddisk : 350 GB
2	Router	1	➤ TP-LINK TD-W8968 ADSL2 + MODEM /300mbps
3	Kabel UTP	1	➤ Cat 5e
4	LAN CARD	2	➤ TP-LINK 100/mbps
5.	Switch	1	➤ HP Procurve 2510-24 J9019B





Gambar 10 Folder Keys Server ClearOS

Konfigurasi koneksi ClearOS Server Pusat dengan ClearOS Server Cabang. Setelah instalasi dan konfigurasi OpenVPN, berikut ini langkah – langkah untuk proses koneksi antara ClearOS server dengan ClearOS client

1. Copy file **Pusat.key** dari ClearOS Server Pusat ke **folder Keys** pada ClearOS Server Cabang selain sebagai pre shared keys antara server pusat dan server cabang, agar data dapat terenskripsi didalam VPN dan ip tunnel server pusat dengan server cabang bisa saling terkoneksi.
2. Aktifkan **OpenVPN** di **ClearOS** Server Pusat dan ClearOS Server Cabang pada menu > **Network** > **VPN** > **OpenVPN**, kemudian pilih **Start** dan **To Automatic** untuk automatic service pada saat awal boot.

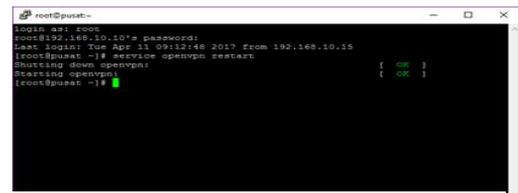


Gambar 11. Aktifasi OpenVPN

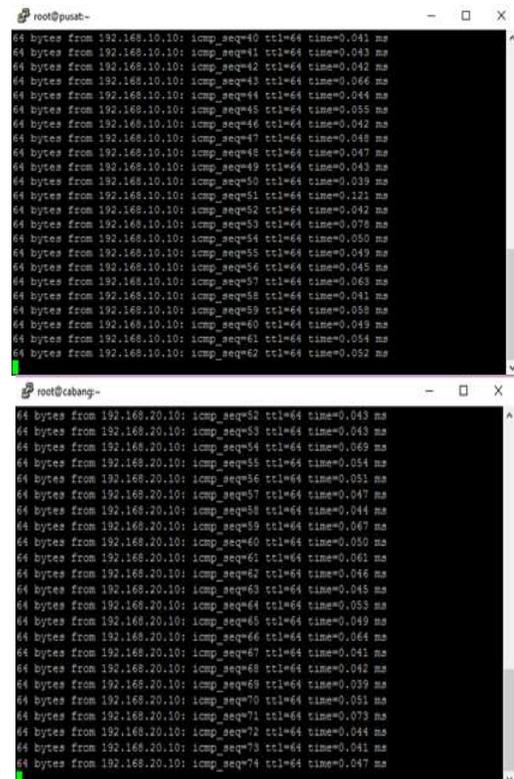
3. Setelah konfigurasi selesai keti perintah **service openvpn restart** melalui putty untuk melihat status dari konfigurasi openvpn di **clients.conf** ok atau failed.

Tes pengujian koneksi jaringan antara kantor pusat dengan kantor cabang

1. Pengujian Koneksi jaringan dari Server kantor pusat dengan Server kantor dapat dilihat pada gambar 12 dan 13

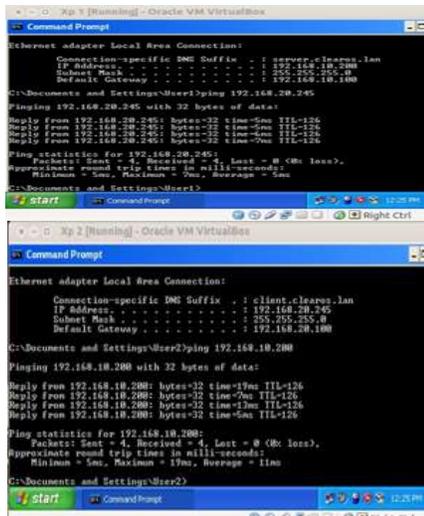


Gambar 12. Service OpenVPN Melalui Putty



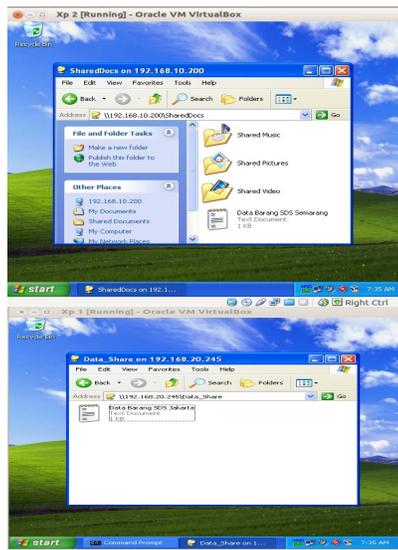
Gambar 13. Koneksi Server Kantor Pusat dengan Server Kantor Cabang

2. Koneksi jaringan dari user kantor pusat dengan user kantor cabang dapat dilihat pada gambar 14



Gambar 14. Koneksi User Kantor Pusat dengan User Kantor Cabang

Tes Pengujian Share data antara kantor pusat dengan kantor cabang dapat dilihat pada gambar 15



Gambar 15. Share Data Antara Kantor Pusat Dengan Kantor Cabang.

## D. PENUTUP

Kesimpulan yang diambil dari perancangan jaringan site to site vpn dengan protocol openvpn di PT. Laris Manis Utama adalah :

1. Berdasarkan lokasi dan informasi data yang diperoleh, maka tipe VPN yang cocok adalah tipe *Site-to-Site* Intranet VPN dengan *Site-to-Site* intranet VPN, jaringan kantor pusat dan kantor cabang terhubung menjadi satu jaringan internal tersendiri. Jenis protocol yang digunakan adalah *OpenVPN* dimana aplikasi tersebut dapat membuat koneksi point-to-point tunnel yang telah terenkripsi. Dimana teknologi yang digunakan untuk enkripsi dalam jaringan *OpenVPN* ini menggunakan teknologi SSL. Dengan enkripsi transfer data hingga 256 bits, *OpenVPN* sangat cocok bagi yang mengutamakan faktor keamanan.
2. Pengalamatan IP pada perancangan jaringan VPN menggunakan IP kelas C. Hal ini disebabkan karena setiap node hanya berjumlah sekitar 30 komputer yang terdapat di kantor pusat sedangkan kantor cabang berjumlah kurang dari 30 komputer. Topologi Jaringan LAN yang digunakan adalah topologi star karena pada topologi ini setiap workstation dikoneksikan pada satu perangkat central, perangkat ini berfungsi untuk mengatur komunikasi data pada setiap workstation. Sehingga mudah dalam mendeteksi error, dan jika salah satu workstation rusak maka perangkat yang rusak tidak mengganggu workstation lain.
3. Pada masing – masing kantor pusat dan kantor cabang dipasang sebuah perangkat PC Server *OpenVPN* dengan *operating system* ClearOS dengan sistem mode gateway, perangkat ini bertindak sebagai embedded gateway dari masing – masing site.

Saran yang diberikan untuk perkembangan dan kemajuan bisnis logistik di PT. Laris Manis Utama, khususnya dalam

kegiatan operasional untuk komunikasi maupun transfer data adalah :

1. Membangun sistem jaringan VPN untuk semua cabang PT. Laris Manis Utama, sehingga akan mempermudah komunikasi transfer data antara pusat dengan cabang.
2. Diharapkan PT. Laris Manis Utama dapat menerapkan rancangan jaringan site to site VPN untuk setiap cabang di PT. Laris Manis Utama, untuk melakukan proses komunikasi transfer maupun komunikasi data agar terkoneksi secara realtime dan dapat melakukan update database pada waktu bersamaan maupun secara berkala dengan aman.
3. Security system yang tertanam dalam server ClearOS kantor pusat maupun kantor cabang.

Kampus dengan Menggunakan Microtic Routerboard, III(2).

- Sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: Alfabeta.
- Sofana, Iwan, (2012) *CISCO CCNA & Jaringan Komputer*. Bandung : Informatika
- Sofana, Iwan. 2013. *Membangun Jaringan Komputer*. Bandung : Informatika.
- Sugeng Winarno, (2015). *Jaringan Komputer Dengan TCP/IP*. Bandung: Modula
- Wendy, and Ahmad Ramadhana. *Membangun VPN Linux Secara Cepat*. Yogyakarta: Andi, 2008.
- Zam, Elvy Zamidra. (2014) *Cara Mudah Membuat Jaringan Wireless*. Jakarta: PT Elex Media Komputindo.

## E. DAFTAR PUSTAKA

- Chaidir, I., & Rino, R. Al. (2019). Implementasi Backup Router Trouble Dengan Metode Virtual Router Redundancy Protocol (VRRP) Pada DISKOMINFO Depok. *Jurnal Ilmu Pengetahuan Dan Teknologi Komputer*, 4(2), 251–257
- Darmawan. (2014), *Metode Penelitian Kuantitatif*. Bandung: Remaja Rosda Karya.
- Gin-Gin Yugianto Oscar Rachman, (2012), *Router Teknologi, Konsep, Konfigurasi, dan Troubleshooting*. Bandung: Informatika
- Gupta, Meeta. (2007) *Building A Virtual Private Network*. USA: Premier Press.
- Ical, (2011), Wordpress. Gerakan Opensource.
- Kurniawan, Bobi. (2014), *Perangkat keras komputer*. Jakarta elex media komputindo
- Silitonga, P., & Morina, I. S. (2014). Analisis QoS (Quality of Service) Jaringan