JURNAL TEKNIK KOMPUTER AMIK BSI

PENERAPAN OPEN VPN IPCOP SEBAGAI SOLUSI PERMASALAHAN JARINGAN PADA PT.KIMIA FARMA TRADING & DISTRIBUTION

Aris Munandar[1], Mohammad Badrul[2]

Abstract*— Computer networks are nothing new at this time. Computer Networks-IP-MPLS VPN is also often the case that resulted in the disruption impede the course of the operations at the company's use. PT. Kimia Farma Trading & Distribution (KFTD) also often experience the same thing, constraints regarding the company's operations caused by the disruption of computer networks-IP-VPN MPLS provider. Facilities and services to the user in a computer network is expected to be given to the maximum so as not interfere and hinder operations, and in the event the user does not need to wait until the computer network-IP-MPLS VPN provider's operational well. With computer networks are created using OpenVPN VPN IPCop can help the user / branches remain operational well. So are useful to the principal (partner company drug providers) in collaboration with PT. Kimia Farma Trading & Distribution (KFTD) that the principal (partner company drug provider) can access to the application to obtain information about the stock of goods of the principal (partner companies drug provider), so that makes it the principal (partner company drug providers) are in getting information.

***Intisari*—** Jaringan komputer bukanlah hal yang baru saat ini. Jaringan komputer VPN-IP-MPLS juga sering terjadi adanya gangguan yang mengakibatkan menghambat jalannya kegiatan operasional pada perusahaan yang menggunakannya. PT. Kimia Farma Trading & Distribution (KFTD) juga sering mengalami hal yang sama, kendala mengenai kegiatan operasional pada perusahaan yang disebabkan oleh gangguan jaringan komputer VPN-IP-MPLS dari provider. Fasilitas dan pelayanan terhadap user dalam jaringan komputer diharapkan dapat diberikan secara maksimal sehingga tidak mengganggu dan menghambat kegiatan operasional, dan apabila terjadi maka user tidak perlu lagi menunggu sampai jaringan komputer VPN-IP-MPLS dari provider beroperasional dengan baik. Dengan jaringan komputer VPN yang dibuat menggunakan OpenVPN IPCop dapat membantu agar user/cabang tetap beroperasional dengan baik. Begitu juga berguna untuk prinsipal (perusahaan rekanan penyedia obat) yang bekerja sama dengan PT. Kimia Farma Trading & Distribution (KFTD) agar prinsipal (perusahaan rekanan penyedia obat) tersebut dapat mengakses ke aplikasi untuk mendapatkan informasi tentang stok barang dari prinsipal (perusahaan rekanan penyedia obat) tersebut, sehingga mempermudah prinsipal (perusahaan rekanan penyedia obat) tersebut dalam mendapatkan informasi.

Kata Kunci: Jaringan Komputer, Virtual Private Network, OpenVPN IPCop

[1,2] Program Studi Teknik Informatika STMIK Nusa Mandiri *Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan. Telp. (021) 78839513 Fax. (021) 78839421; e-mail:niris211206@gmail.com; mohammad.mbl@nusamandiri.ac.id*

I. PENDAHULUAN

Jaringan komputer memberikan kemampuan sebagai media komunikasi yang dapat mempercepat proses kerja baik dari segi waktu maupun ruang. Selain itu teknologi informasi dapat mempermudah dalam mengakses sebuah informasi. Sehingga perkembangan teknologi informasi sangat berpengaruh dalam segala kehidupan manusia. Jaringan memungkinkan kelompok-kerja berkomunikasi dengan lebih efisien. Surat dan penyampaian pesan elektronik merupakan substansi sebagian besar sistem jaringan, disamping sistem penjadwalan, pemantauan proyek, konferensi online dan groupware, dimana semuanya membantu team bekerja lebih produktif.

Namun Jaringan komputer juga sering terjadi adanya gangguan yang mengakibatkan menghambat jalannya kegiatan operasional pada perusahaan yang menggunakannya. Sama seperti yang dialami oleh PT. Kimia Farma Trading & Distribution (KFTD) juga sering mengalami hal yang sama, kendala mengenai kegiatan operasional pada perusahaan yang disebabkan oleh gangguan jaringan komputer dari provider.

Teknologi jaringan yang dapat mendukung hal ini adalah teknologi *Virtual Private Network* (VPN), yang dapat mengemulasikan dua jaringan yang lokasinya berjauhan untuk saling berkomunikasi seakan-akan kedua jaringan tersebut di dalam suatu jaringan internet yang besar.

Salah satu solusi yang ditawarkan adalah dengan menggunakan VPN [1]. VPN adalah sebuah koneksi *virtual* yang bersifat privat, disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan *virtual* VPN Menghubungkan PC dengan jaringan public atau *internet* namun sifatnya privat, karena bersifat privat maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya".

Virtual Private Network(VPN) dikembangkan untuk membangun sebuah intranet dengan jangkauan yang luas melalui jaringan internet. Intranet sudah menjadi suatu komponen penting dalam suatu perusahaan dewasa ini. VPN dapat digunakan sebagai alat komunikasi oleh kantor Pusat dan kantor Cabang. Dengan dibantu perangkat lunak atau suatu alat khusus. *Virtual Private Network* atau VPN merupakan teknologi yang diterapkan pada suatu institusi atau perusahaan yang membutuhkan akses ke suatu jaringan lokal secara aman. Teknologi yang digunakan adalah internet yang kemudian diautentikasi pada server VPN untuk melakukan

hubungan secara lokal terhadap server tersebut. Teknologi ini sangat tepat bagi perusahaan yang memiliki banyak cabang yang tersebar di setiap provinsi.

Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau rute, namun didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan pengguna-pengguna yang ditunjuk ke akses VPN dan informasi yang mengalir melaluinya.VPN bukanlah hal baru, yang membuat VPN ini menjadi menarik adalah dikarenakan kemampuannya untuk mengamankan Intranet dengan kedinamisannya untuk mengakomodasi lingkungan bisnis yang selalu berubah-ubah pesat.

OpenVPN adalah salah satu jenis aplikasi penyedia layanan VPN yang gratis. OpenVPN menggunakan SSL untuk menangani tunneling. OpenVPN memiliki dukungan yang luas terhadap berbagai macam produk-produk opensource, terutama untuk aplikasi-aplikasi yang menangani proses enkripsi SSL/TLS dan Otentikasi. Secara default, OpenVPN menggunakan library OpenSSL untuk membangun tunnel.

II. KAJIAN LITERATUR

Jaringan komputer adalah "Sebuah sistem yang terdiri atas komputer, *software* dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama"[2]. Secara lebih sederhana, jaringan komputer dapat diartikan sebagai sekumpulan komputer beserta mekanisme dan prosedurnya yang saling terhubung dan berkomunikasi. Komunikasi yang dilakukan oleh komputer tersebut dapat berupa transfer berbagai data, instruksi, dan informasi dari satu komputer ke komputer lain.

Dibandingkan dengan komputer yang berdiri sendiri (*stand-alone*), jaringan komputer memiliki beberapa keunggulan antara lain:

a. Berbagi peralatan dan sumber daya
   Beberapa komputer dimungkinkan untuk saling memanfaatkan sumber daya yang ada, seperti printer, harddisk, serta perangkat lunak bersama, seperti aplikasi perkantoran, basis data (database), dan sistem informasi. Penggunaan perangkat secara bersama ini akan menghemat biaya dan meningkatkan efektivitas peralatan tersebut [3].
b. Integrasi data
   Jaringan komputer memungkinkan pengintegrasian data dari atau ke semua komputer yang terhubung dalam jaringan tersebut [3].
c. Komunikasi
   Jaringan komputer memungkinkan komunikasi antar pemakai komputer, baik melalui e-mail, teleconference dan sebagainya [3]
d. Keamanan (Security)
   Jaringan komputer mempermudah dalam pemberian perlindungan terhadap data. Meskipun data pada sebuah komputer dapat diakses oleh komputer lain, tetapi kita dapat membatasi akses orang lain terhadap data tersebut. Selain itu kita juga bisa melakukan pengamanan terpusat atas seluruh komputer yang terhubung ke jaringan [3].

Jaringan komputer akan memberikan layanan yang berbeda kepada perorangan dirumah-rumah dibandingkan dengan layanan diberikan oleh perusahaan. Terdapat tiga hal pokok yang menjadi daya tarik jaringan komputer pada perorangan yaitu :

1. *Access* ke informasi yang berada di tempat lain (seperti akses berita hari ini, info *e-government, e-commerce atau e-business*), semuanya *uptodate* [4].
2. Komunikasi orang ke orang (*person to person* seperti *e-mail, chatting, video conference*) [4].
3. Hiburan interaktif (seperti nonton tv *on-line*, radio *streaming*, *download* film atau lagu) [4].

A. LAN

Local Area Network (LAN) adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolahan atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 *Ethernet* menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi *Ethernet*, saat ini teknologi 802.11b (atau biasa disebut Wi-fi) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi Wi-fi biasa disebut *hotspot* [2].

B. MAN

MAN adalah sebuah jaringan komputer besar yang mencangkup sebuah kota atau sebuah kampus besar. MAN biasanya merupakan gabungan dari LAN yang menggunakan teknologi *backbone* berkecepatan tinggi dan menyediakan layanan ke jaringan yang lebih besar seperti WAN dan *Internet* [5]. *Metropolitan Area Network* (MAN) suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya[2]. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antara 10 hingga 50 km, MAN ini merupakan jaringan yang tepat untuk membangun jaringan antara kantor-kantor dalam suatu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya, prinsip sama dengan LAN, hanya saja jarak lebih luas, yaitu 10-50 km

C. WAN

Suatu WAN meliputi area geografi yang lebih luas lagi, yang meliput suatu negara atau dunia. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda. WAN digunakan untuk menghubungkan banyak LAN yang secara gografis terpisah. WAN dibuat dengan cara menghubungkan LAN menggunakan layannan seperti Leased Line, dial-up, satelit atau layanaan paket carrier. Dengan WAN, sekolah yang ada di Yogyakarta dapat berkomunikasi dengan sekolah yang ada di Munchen Jerman dalam beberapa menit saja tanpa mengeluarkan biaya yang banyak[5]. *Wide Area Network*

(WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota, atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan computer dilokasi yang lain[2].

D. IP ADDRESS

IP Address merupakan singkatan dari *Internet Protocol Address*, *IP Address* adalah identitas numeric yang diberikan kepada suatu alat seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protokol sebagai sarana komunikasi, *IP Address* memiliki dua fungsi yaitu (Winarto, Zaki, & Community, 2013) :

1. Sebagai alat identifikasi host atau antarmuka pada jaringan.
2. Sebagai alamat lokasi jaringan.

IP Address sendiri memakai system bilangin 32 bit, system ini dikenal dengan nama *Internet Protocol* version 4 atau IPv4. Saat ini IPv4 masih ramai digunakan, untuk memudahkan dalam pembagiannya maka *IP Address* dibagi ke dalam kelas-kelas yang berbeda, yaitu sebagai berikut[6] :

1. Kelas A
   IP Address kelas *A* terdiri atas 8 bit untuk network ID dan sisanya 24 bit digunakan untuk host ID, sehingga *IP Address* kelas A digunakan untuk jaringan dengan jumlah host sangat besar. Pada bit pertama diberikan angka 0 sampai dengan 127[6].
2. Kelas B
   IP Address kelas *B* terdiri atas 16 bit untuk network ID dan sisanya 16 bit digunakan untuk host ID, sehingga *IP Address* kelas B digunakan untuk jaringan dengan jumlah host tidak terlalu besar. Pada 2 bit pertama, diberikan angka 10 [6].
3. Kelas C
   IP Address kelas *C* terdiri atas 24 bit untuk network ID dan sisanya 8 bit digunakan untuk host ID, sehingga *IP Address* kelas C digunakan untuk jaringan berukuran kecil. Kelas C biasanya digunakan untuk jaringan *Local Area Network* atau LAN. Pada 3 bit pertama, diberikan angka 110 [6].

Kelas *IP Address* lainnya adalah D dan E, namun kelas IP D dan E tersebut tidak digunakan untuk alokasi IP secara normal tetapi digunakan untuk *IP multicasting* dan untuk eksperimental [6].

Nilai *subnet mask* berfungsi untuk memisahkan *network ID* dengan *host ID*. Subnet mask diperlukan oleh TCP/IP untuk menentukan, apakah jaringan yang dimaksud adalah jaringan lokal atau nonlokal. Untuk jaringan Nonlokal berarti TCP/IP harus mengirimkan paket data melalui sebuah Router. Dengan demikian, diperlukan *address mask* untuk menyaring *IP Address* dan paket data yang keluar masuk jaringan tersebut [6].

Network ID dan host ID didalam *IP Address* dibedakan oleh penggunaan subnet mask. Masing-masing subnet mask menggunakan pola nomor 32-bit yang merupakan *bit groups* dari semua satu (1) yang menunjukkan *network ID* dan semua nol (0) menunjukkan *host ID* dari porsi *IP Address* [7].

E. VOIP

VPN adalah Virtual, karena tidak ada koneksi jaringan langsung nyata antara dua (atau lebih) mitra komunikasi[8], tetapi hanya koneksi virtual yang disediakan oleh VPN Software, biasanya melalui koneksi Internet publik. Pribadi, karena hanya anggota perusahaan terhubung oleh Software VPN yang diizinkan untuk membaca data yang ditransfer. Pada VPN terdapat 3 mekanisme penting, yaitu enkripsi, autentikasi dan autorisasi.

Enkripsi merupakan proses mengubah data ke dalam bentuk yang hanya bisa dibaca oleh penerima yang diinginkan. Untuk membaca pesan yang telah dienkripsi tersebut, penerima data harus mempunyai kunci dekripsi yang benar. *Public-key encryption* menggunakan dua kunci. Satu kunci dikenal sebagai *public key*, yang oleh setiap orang boleh gunakan selama enkripsi dan dekripsi. Walaupun nama kuncinya adalah *public key*, kunci ini dipunyai oleh sebuah entiti. Jika entiti kedua perlu untuk berkomunikasi dengan pemilik kunci, entiti kedua menggunakan *public key* untuk melakukan komunikasi itu. *Public key* mempunyai *corresponding private key. Private key* adalah key yang bersifat pribadi kepada entiti. Sebagai hasilnya, dengan enkripsi *public key* setiap orang dapat menggunakan pemilik *public key* unyuk mengenkripsi dan mengirim pesan. Tetapi, hanya pemilik yang mempunyai *private key* untuk mendekripsi pesan. Dalam berkomunikasi, pengirim menggunakan *public key*-nya untuk mengenkripsi pesan. Penerima menerima pesan dan mendekripsi pesan yang telah didecode menggunakan *private key*. *Pretty Good Privacy* (PGP) dan *Data Encryption Standard* (DES) adalah dua dari *public key* enkripsi yang paling populer.

Autentikasi merupakan proses untuk memastikan data dikirim kepada penerima yang diinginkan. Sebagai tambahan, autentikasi juga memastikan integritas penerima dari pesan dan sumbernya. Dalam bentuk yang paling sederhana, autentikasi memerlukan paling sedikit *username* dan *password* untuk menerima akses ke sumber spesifik. Dalam bentuk yang kompleks, autentikasi dapat didasari dari *secret-key encryption* atau *public-key encryption*. Autorisasi merupakan proses memberikan atau menolak akses ke sumber yang berlokasi dalam jaringan setelah pengguna telah berhasil diidentifikasi dan diautentiksi.

Pada VPN juga terdapat protokol yang disebut dengan *VPN Tunneling Protocols*, protokol-protokol ini berguna untuk memastikan aspek keamanan dari transaksi melalui VPN. Protokol yang biasa digunakan, yaitu *IP Security* (IPSec), *Point-to-Point Tunneling Protoco*l (PPTP), *Layer 2 Tunneling Protocol* (L2TP), dan protokol-protokol lainnya seperti SSL/TLS. *IP Security* (IPSec). Dikembangkan oleh IETF, IPSec adalah standar terbuka yang memastikan keamanan trasmisi dan autentikasi pengguna melalui jaringan

publik. Tidak seperti teknik enkripsi lainnya, IPSec beroperasi pada *Network Layer* dari model tujuh layer OSI. Oleh karena itu, dapat diimplementasikan secara bebas ke aplikasi yang berjalan melalui jaringan. Sebagai hasilnya jaringan dapat diamankan tanpa perlu mengimplementasikan dan mengkoordinasi keamanan untuk setiap aplikasi.

IP Security (IPSec). Dikembangkan oleh IETF, IPSec adalah standar terbuka yang memastikan keamanan trasmisi dan autentikasi pengguna melalui jaringan publik. Tidak seperti teknik enkripsi lainnya, IPSec beroperasi pada *Network Layer* dari model tujuh layer OSI. Oleh karena itu, dapat diimplementasikan secara bebas ke aplikasi yang berjalan melalui jaringan. Sebagai hasilnya jaringan dapat diamankan tanpa perlu mengimplementasikan dan mengkoordinasi keamanan untuk setiap aplikasi.

Point-to-Point Tunneling Protocol (PPTP). Dikembangkan oleh Microsoft, 3COM, dan Ascenf Communicarions, PPTP dimaksudkan sebagai alternatif untuk IPSsec. Tetapi, IPSec masih menjadi favorit tunneling protokol. PPTP beroperasi pada layer kedua (*Data Link Layer*) dari model OSI dan digunakan untuk mengamankan transmisi dari trafik Windows.

Layer 2 Tunneling Protocol (L2TP). Dikembangkan oleh Cisco System, L2TP juga dimaksudkan untuk mengganti IPSec sebagai tunneling protocol. Tetapi IPSec masih terus-menerus menjadi protokol yang dominan untuk komunikasi yang aman melalui *internet.* L2TP adalah kombinasi dari *layer 2forwarding* (L2F) dan PPTP dan digunakan untuk mengenkapsulasi *frame Pointto- Point Protocol* (PPP) yang dikirim melalui X.25, FR, dan jaringan ATM.

Faktor lain yang membedakan antara sistem dan protokol yang dijelaskan di atas adalah:

1. Ketersediaan dari mekanisme autentikasi
2. Mendukung untuk fitur *advanced networking* seperti *Network Address Translation* (NAT)
3. Alokasi dinamis dari IP address untuk partner tunnel dalam mode dial-up
4. Mendukung untuk *Public Key Infrastructures* (PKI)

VPN sendiri memiliki beberapa tipe, VPN yang biasa dikenal adalah *Remote-Access VPN* dan *Site-to-Site VPN*.

III. METODE PENELITIAN

Dalam memudahkan pembuatan dan pengumpulan data-data yang diperlukan dalam penelitian ini, maka penulis menggunakan metode penelitian sebagai berikut :

1. Teknik Pengumpulan Data

Teknik yang dilakukan untuk pengumpulan data adalah sebagai berikut :

a. Observasi
   Yaitu melakukan pengamatan langsung dilapangan untuk mendapatkan data-data yang dibutuhkan untuk penulisan penelitian ini.
b. Wawancara
   Metode ini dilakukan dengan cara tanya jawab secara langsung dengan administrator jaringan untuk mendapat data-data yang lebih rinci lagi mengenai jaringan yang ada di PT. Kimia farma.
c. Studi Pustaka
   Metode ini merupakan cara untuk mendapatkan data-data secara teoritis sebagai bahan penunjang dalam penyusunan penelitian dengan cara mempelajari, meneliti dan menelaah berbagai literatur-literatur dari perpustakaan maupun dari buku-buku referensinya lainnya, juga dari situs-situs internet yang berkaitan dengan topik penelitian.

2. Analisa Penelitian

Analisa penelitian yang dilakukan terdiri dari :

a. Analisa Kebutuhan
   Dalam analisa kebutuhan ini penulis mencoba menyiapkan analisa kebutuhan dalam merancang jaringan VPN dengan OpenVPN IPCop baik hardware maupun software yang akan di gunakan.
b. Desain
   Dalam metode ini penulis membuat analisa desain jaringan yang digunakan untuk penerapan *VPN-IP COP*.
c. Testing
   Melakukan testing, meliputi tes koneksi dan juga test keamanan untuk memastikan semuanya agar jaringan VPN sesuai yang diharapkan sebelum diimplementasikan. Dengan menginstal aplikasi OpenVPN *client* di setiap user yang akan menggunakan jaringan OpenVPN ini. Serta mengeset sertifikat di server IPCop agar dapat terhubung.
d. Implementasi
   Dalam tahap implementasi ini, penulis melakukan percobaan tentang VPN-IP Cop kepada beberapa prinsipal (perusahaan rekanan penyedia obat) dan cabang-cabang PT. Kimia Farma Trading & Distribution (KFTD) yang terkait dengan aplikasi, agar dapat terintegrasi ke aplikasi dari PT. Kimia Farma Trading & Distribution (KFTD)..

IV. HASIL DAN PEMBAHASAN

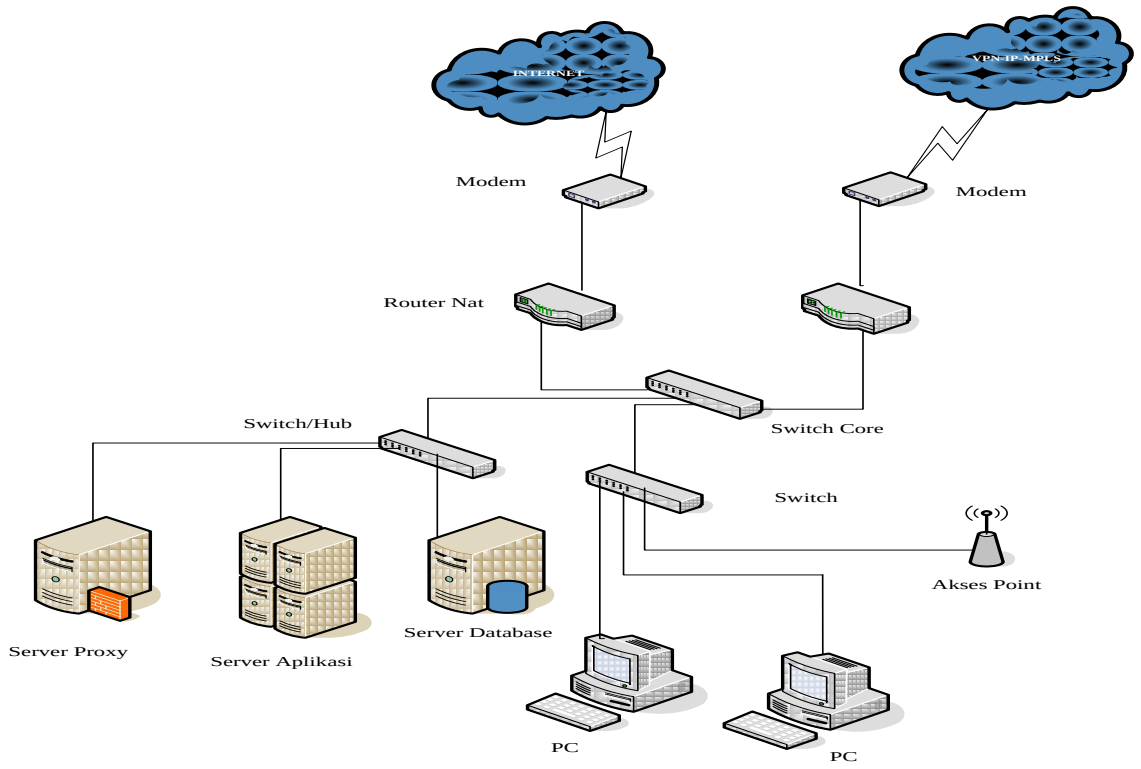
Dalam pembahasan ini penulis membahas tentang jaringan yang sedang diterapkan di perusahaan dan usulan jaringan yang penulis usulkan.

A. Jaringan yang sedang diterapkan

Pembahasan ini penulis akan membahas tentang topologi jaringan, arsitektur jaringan, skema jaringan dan keamanan jaringan

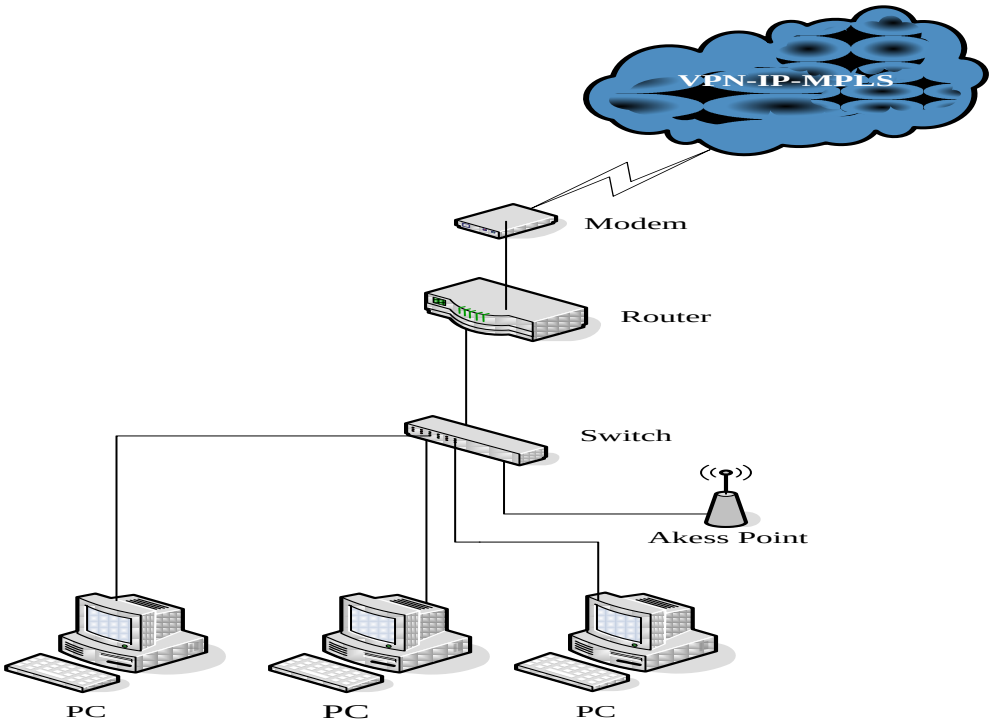
1. Topologi jaringan

Pada PT. Kimia Farma Trading & Distribution (KFTD) mengunakan topologi star karena seluruh PC terkoneksi pada switch, protokol jaringan yang digunakan adalah TCP/IP, seluruh NIC yang di gunakan mendukung kecepatan 10/100/1000 Mbps. Pada kantor cabang topologi yang di pakai juga menggunakan topologi star hal ini karna lebih memudahkan pada saat proses instalasi perangkat yang di butuhkan pada jaringan tersebut.



Sumber : Hasil Penelitian (2014)

Gambar 1. Topologi Jaringan Kantor Pusat



Sumber : Hasil Penelitian (2014)

Gambar 2. Topologi Jaringan Kantor Cabang

2. Arsitektur Jaringan

Arsitektur jaringan yang digunakan, IP Addres Jaringan dan Fungsi Arsitektur jaringan model OSI (*Open System Interconnection*) atau TCP/IP serta gambaran Topologi secara keseluran dari jaringan tersebut. Berikut ip address yang digunakan.

Tabel 1. IP Address Jaringan Pusat

Jenis IP	IP Address
Router Nat	192.168.xxx.xxx
Router	172.16.xxx.xxx
Subnetmask	255.255.xxx.xxx
Server Database	10.9.xxx.xxx
Server Aplikasi	10.9.xxx.xxx
Server Proxy	10.9.xxx.xxx
Gateway Server	10.9.xxx.xxx
Gateway Client	192.168.xxx.xxx
DNS Server	10.9.xxx.xxx
Access Point 1	192.168.xxx.xxx
Client (LAN)	192.168.xxx.xxx s/d 192.168.xxx.xxx
Client (Wireless)	192.168.xxx.xxx s/d 192.168.xxx.xxx

Sumber : Hasil Penelitian (2014)

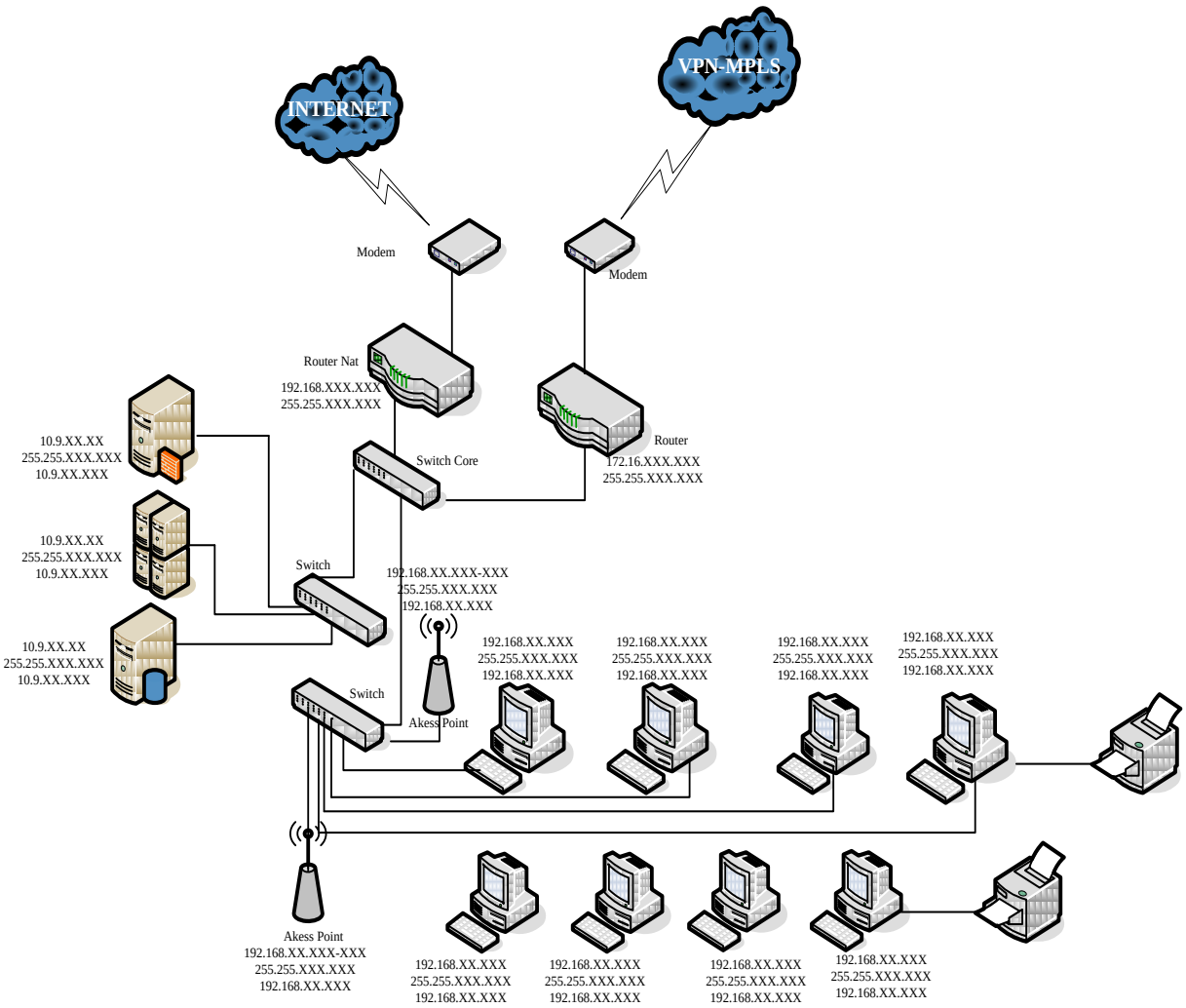
Tabel 2. IP Address Jaringan Cabang

Jenis IP	IP Address
Router	192.168.xxx.xxx
Gateway	192.168.xxx.xxx
DNS Server	10.9.xxx.xxx
Subnetmaks	255.255.xxx.xxx

Sumber : Hasil Penelitian (2014)

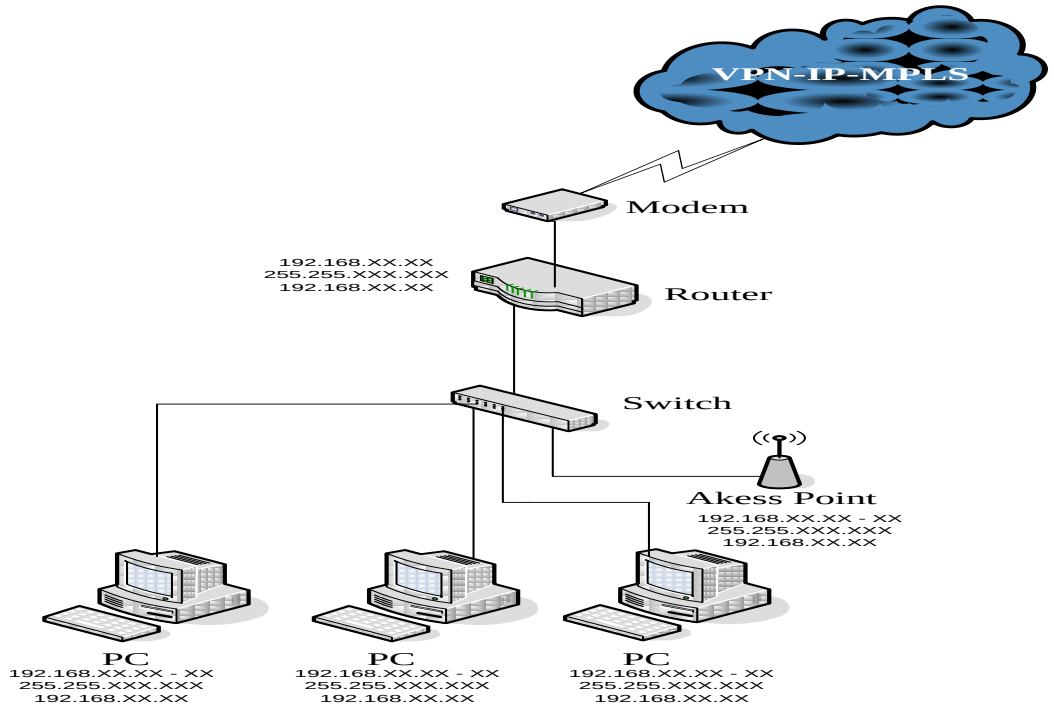
3. Skema Jaringan

Berikut ini adalah skema jaringan pusat dan skema jaringan pada kantor cabang di PT. Kimia Farma Trading & Distribution.



Sumber : Hasil Penelitian (2014)

Gambar 3. Skema Jaringan Kantor Pusat



Sumber : Hasil Penelitian (2014)

Gambar 4. Skema Jaringan Kantor Cabang

4. Keamanan Jaringan

Sistem keamanan yang diterapkan baik pada kantor pusat maupun kantor cabang, bertumpu pada PC *Router*. Sedangkan pada sisi *client* terpasang *software antivirus*. *Antivirus* berfungsi untuk mencegah penyebaran *virus* yang datangnya dari *client*. Penyeberan ini pada umumnya berasal dari pertukaran data melalui USB *flashdisk* atau media penyimpanan lainnya antivirus yang digunakan untuk server adalah Kaspersky for Server. Sedangkan untuk client Kaspersky for Client. Proxy Server berfungsi untuk membatasi karyawan/user untuk membuka situs-situs/URL-URL tertentu yang dapat mengganggu kinerja dari karyawan/user.

B. Jaringan Usulan dari Penulis

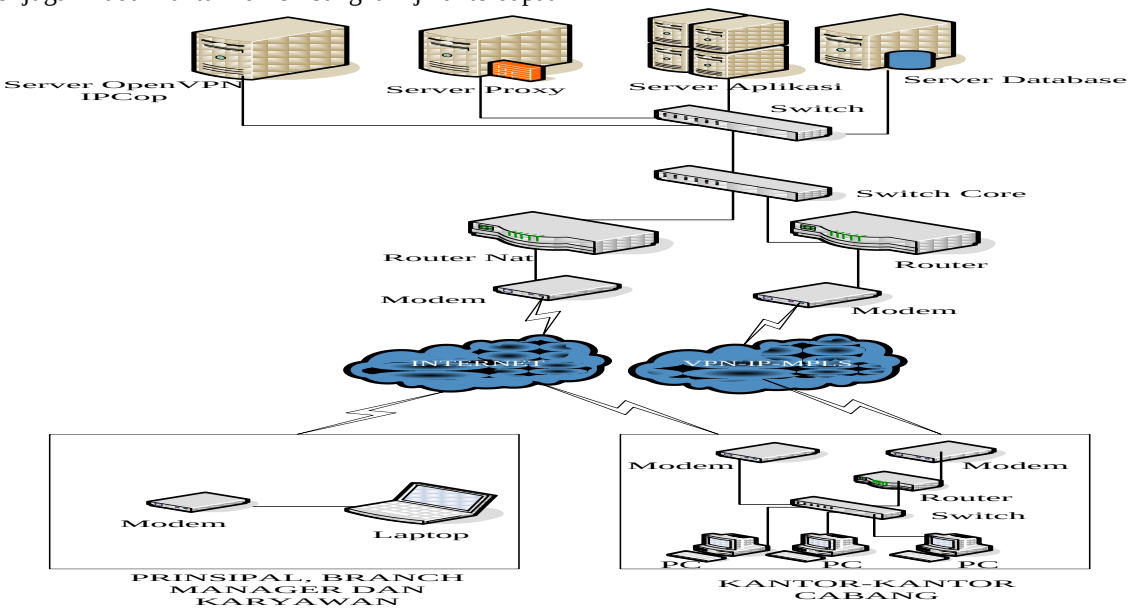
Jaringan komputer bukanlah hal yang baru saat ini. Hampir disetiap Perusahaan terdapat jaringan komputer untuk memperlancar arus informasi didalam perusahaan tersebut. Namun Jaringan komputer juga sering terjadi adanya gangguan yang mengakibatkan menghambat jalannya kegiatan operasional pada perusahaan yang menggunakannya. Sama seperti yang dialami oleh PT. Kimia Farma Trading & Distribution (KFTD) juga sering mengalami hal yang sama, kendala mengenai kegiatan operasional pada perusahaan yang disebabkan oleh gangguan jaringan komputer dari provider. Selain adanya masalah pada jaringan dari provider ada juga kendala masalah dari prinsipal (perusahaan rekanan penyedia obat) yang bekerja sama pada PT. Kimia Farma Trading & Distribution (KFTD) yang kesulitan untuk mendapatkan informasi tentang laporan stok barang dari prinsipal (perusahaan rekanan penyedia obat) tersebut yang dicabang-cabang PT. Kimia Farma Trading & Distribution (KFTD), karena aplikasi hanya bisa dibuka menggunakan jaringan komputer yang terintegrasi oleh jaringan komputer pada PT. Kimia Farma Trading & Distribution (KFTD).

Solusi yang diberikan untuk menghadapi permasalahan yang sedang dihadapi oleh PT. Kimia Farma Trading & Distribution adalah dengan menggunakan teknologi *Virtual Private Network* (VPN) Menggunakan OpenVPN IPCop, karena dengan *Virtual Private Network* (VPN) Menggunakan OpenVPN IPCop dapat membantu agar user/cabang tetap beroperasional dengan baik. Begitu juga berguna untuk prinsipal (perusahaan rekanan penyedia obat) yang bekerja sama dengan PT. Kimia Farma Trading & Distribution (KFTD) agar prinsipal (perusahaan rekanan penyedia obat) tersebut dapat mengakses ke aplikasi untuk mendapatkan informasi tentang stok barang dari prinsipal (perusahaan rekanan penyedia obat) tersebut, sehingga mempermudah prinsipal (perusahaan rekanan penyedia obat) tersebut dalam mendapatkan informasi.

1. Topologi Jaringan usulan

Proses bisnis yang sekarang sedang berjalan pada PT. Kimia Farma Trading & Distribution (KFTD), kantor-kantor cabang melalukan operasional sehari-hari dengan terhubung aplikasi bisnis yang terdapat dikantor pusat. Walaupun kadang-kadang terjadi gangguan operasional yang diakibatkan oleh gangguan dari provider yang bekerja sama untuk mengatasi hal ini perlu adanya koneksi jaringan alternatif agar cabang tetap beroperasional. Dengan adanya jaringan VPN menggunakan OpenVPN IPCop, masing-masing kantor cabang dapat berjalan dan beroperasional seperti biasanya.

Kantor pusat merupakan *central site (star)* dan kantor-kantor cabang sebagai *remote office (spokes).* Topologi *star* dan *spokes* juga mudah untuk dikembangkan jika terdapat kantor-kantor cabang yang baru dari berbagai kota yang ingin dihubungkan dengan kantor pusat.

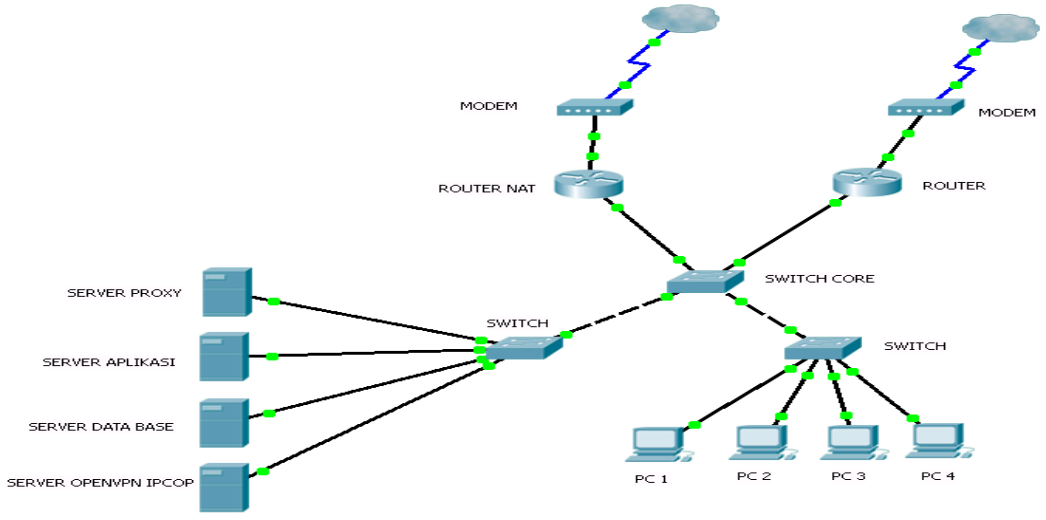


Sumber : Hasil Penelitian (2014)

Gambar 5. Topologi jaringan usulan

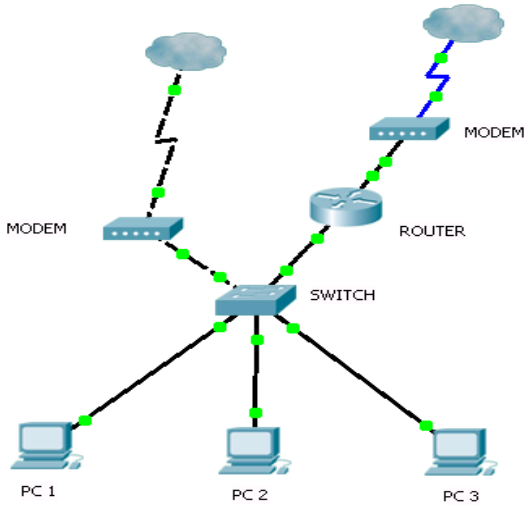
2. Skema Jaringan Usulan

Dengan adanya rancangan VPN menggunakan OpenVPN IPCop yang baru ini, perlu dilakukan beberapa perubahan pada jaringan kantor pusat PT. Kimia Farma Trading & Distribution (KFTD) adanya penambahan server dan ip publik. Jaringan pada kantor pusat akan dibagi menjadi dua bagian, yaitu jaringan yang dapat menggunakan jaringan MPLS dari provider dan jaringan yang VPN menggunakan OpenVPN IPCop (digunakan untuk yang berada diluar kantor). Pembagian jaringan dilakukan agar aplikasi yang digunakan dapat tetap di akses oleh cabang-cabang, prinsipal (perusahaan rekanan penyedia obat) dan kepala cabang yang tidak terkoneksi atau terhubung dengan jaringan MPLS yang bekerja sama dengan PT. Kimia Farma Trading & Distribution (KFTD) untuk mengakses dan terhubung ke aplikasi yang disediakan oleh kantor pusat, mengingat aplikasi yang digunakan merupakan aplikasi online ke kantor pusat, maka seluruh cabang harus bisa terkoneksi ke aplikasi tersebut agar bisa tetap beroperasional untuk melayani pelanggan-pelanggan atau customer yang ada pada kantor-kantor cabang.



Sumber : Hasil Penelitian (2014)

Gambar 6. Skema jaringan usulan kantor pusat



Sumber : Hasil Penelitian (2014)

Gambar 7. Skema jaringan usulan kantor cabang

3. Keamanan Jaringan

Sistem keamanan yang diterapkan baik pada kantor pusat maupun kantor cabang, bertumpu pada PC *Router*. Sedangkan pada sisi *client* terpasang *software antivirus*. *Antivirus* berfungsi untuk mencegah penyebaran *virus* yang datangnya dari *client*. Penyeberan ini pada umumnya berasal dari pertukaran data melalui USB *flashdisk* atau media penyimpanan lainnya antivirus yang digunakan untuk server adalah Kaspersky for Server. Sedangkan untuk client Kaspersky for Client Kaspersky Endpoint Security 8. Firewall yang berfungsi untuk mengamankan IPCop dari serangan, salah satunya dengan mematikan fitur respon terhadap ping ke interface IPCop.

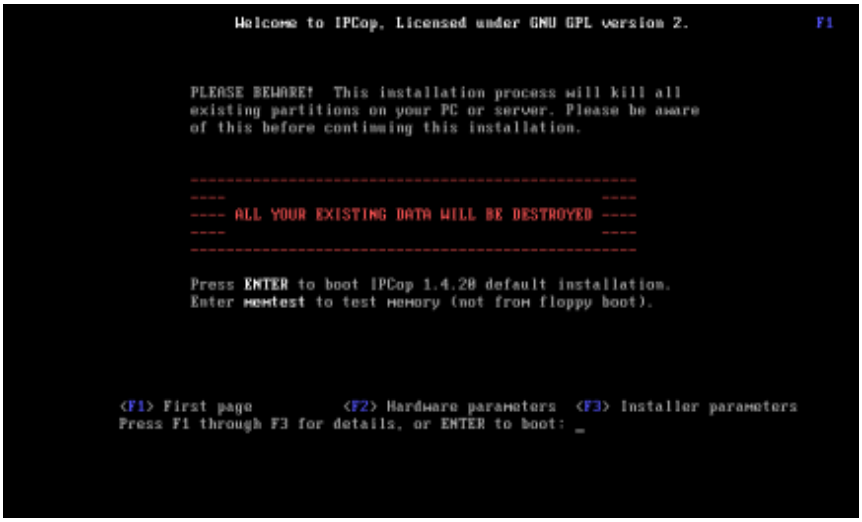
4. Perancangan Aplikasi

Pada perancangan aplikasi penulis akan menjelaskan langka-langkah instalasi dan konfigurasi untuk membangun jaringan *virutal private tenwork.* menggunakan OpenVPN IPCop ada beberapa hal yang harus dilakukan yaitu :

1. Instalasi IPCop

Langkah-langkah yang dilakukan dalam proses instalasi IPCop OS adalah sebagai berikut:

a. Burning terlebih dahulu kedalam CD-R ipcop-1.4.20.iso.
b. Setting bios anda, agar dapat booting CD-ROM terlebih dahulu.
c. Masukan CD-R yang sudah berisikan ipcop-1.4.20.iso hasil *burning* dari step yang pertama.
d. Seteleh menunggu sejenak dari proses booting maka akan keluar proses pilihan paket-paket yang ingin kita install, tekan “enter” untuk melanjuk kan proses installasi.

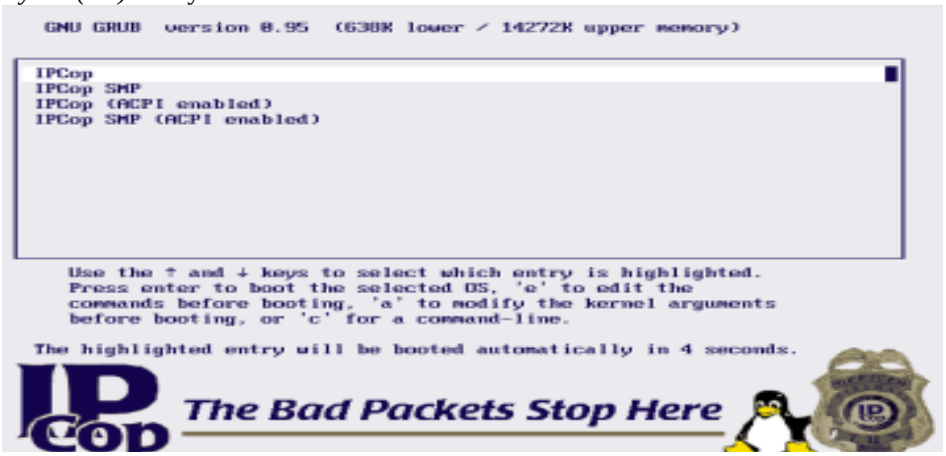


Sumber : Hasil Penelitian (2014)

Gambar 8. Gambar Booting Awal IPCop

e. Pada tahap ini ikuti proses penginstalasian seperti instalasi *operating sytem (OS)* lainnya.

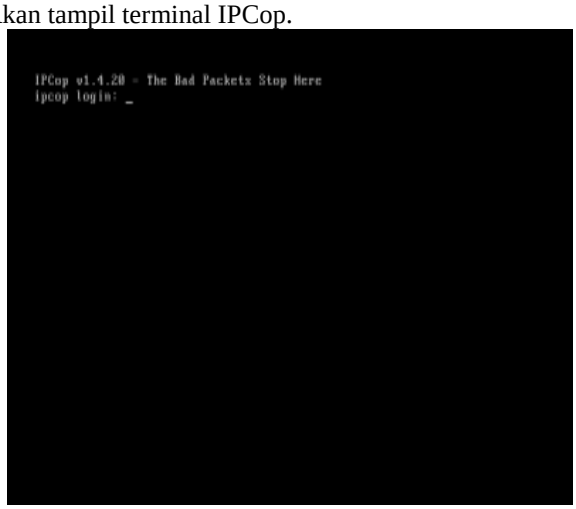
f. Pada tahap ini setelah proses instalasi yang kita lakukan telah selesai tekan "ok" untuk reboot.



Sumber : Hasil Penelitian (2014)

Gambar 9. Gambar Booting IPCop

g. Setelah komputer booting kembali ke ipcop-1.4.20. Akan tampil terminal IPCop.



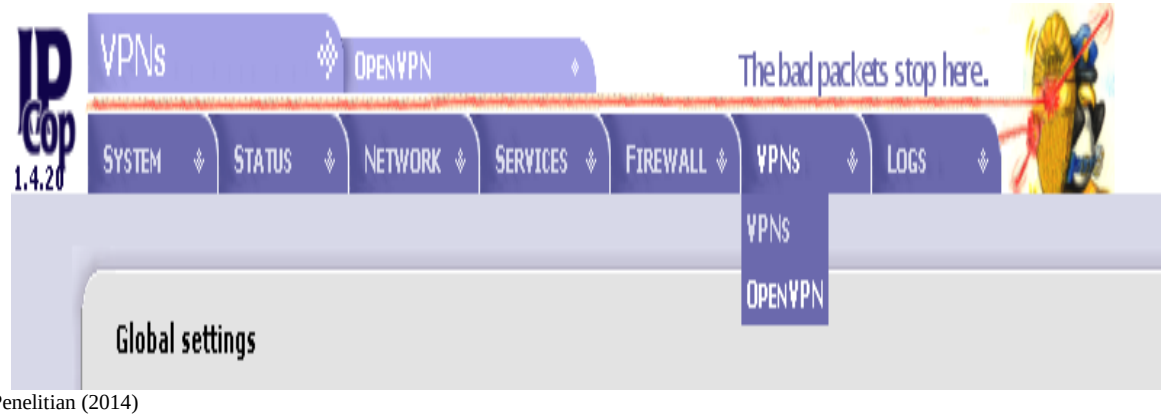
Sumber : Hasil Penelitian (2014)

Gambar 10. Terminal IPCop

2. Konfigurasi OpenVPN di IPCop

Menginstal OpenVPN di IPCop membutuhkan sebuah addons, addons yang digunakan untuk menginstal dan membuat IPCop memiliki fasilitas OpenVPN server adalah addons yang bernama zerina.

a. Download file ZERINA-0.9.5b-Installer.tar.gz.
b. Salin *file* ZERINA-0.9.5b-Installer.tar.gz ke direktori pada Server IPCop.
c. Lakukan remote ke server IPCop dengan menggunakan ssh atau putty.
d. Lakukan extract file ZERINA-0.9.5b-Installer.tar.gz dengan cara ketik tar xvfz ZERINA-0.9.5b-Installer.tar.gz.
e. Lalu masuk direktori zerina-0.9.5b, untuk proses instalasi ketik perintah ./install.
f. Setelah proses instalasi selesai, menu addons Zerina OpenVPN akan tampil pada menu VPNs.



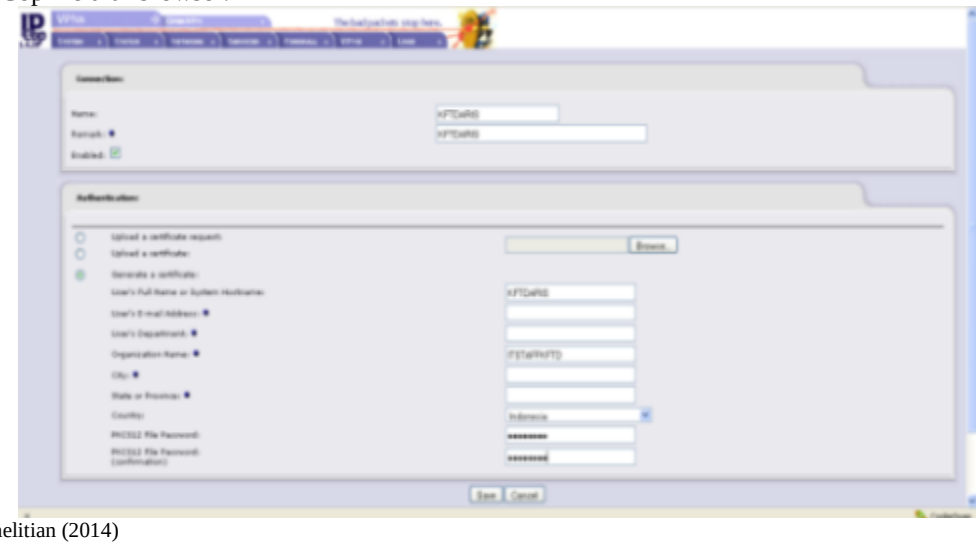
Sumber : Hasil Penelitian (2014)

Gambar 11. Konfigurasi submenu openVPN

3. Pembuatan Sertifikat

Proses installasi addons OpenVPN pada server IPCop maka proses yang dilakukan yaitu membuat sertifikat untuk *client*.

a. Masuk server IPCop melalui browser.



Sumber : Hasil Penelitian (2014)

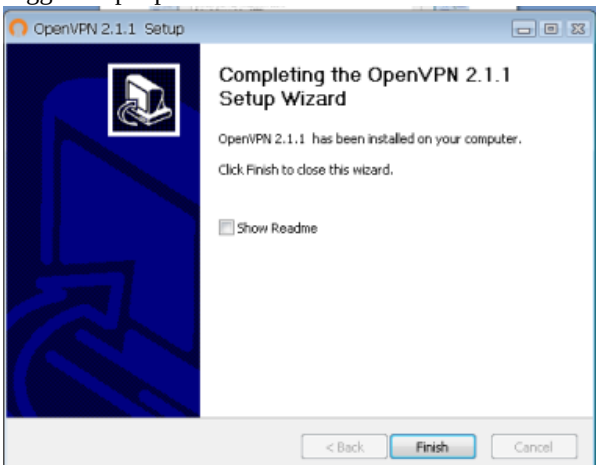
Gambar 12. Gambar Seting User

b. Pilih tab VPNs.
c. Lalu pilih add.
d. Pilih *type connection*, lalu klik tombol add.
e. Masukkan *client* atau user yang akan di tambah untuk konksi ke server.

4. Instalasi OpenVPN Client

Proses instalasi *OpenVPN Client, openVPN Client* ini berfungsi untuk menghubungkan antara *client* dengan server IPCop.

a. Siapkan file aplikasi *openVPN client.*
b. Lakukan proses instal *openVPN client* seperti menginstal aplikasi lainnya.
c. Tunggu sampai proses instalasi selesai.
d. Jika ada permintaan untuk menginstal menginstal driver tambahan klik *continue anyway.*
e. Tunggu sampai proses instalasi selesai.



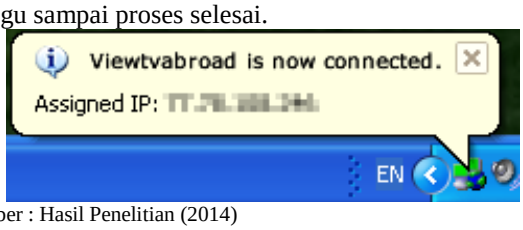
Sumber : Hasil Penelitian (2014)

Gambar 13. Gambar Seting User

5. Konfigurasi OpenVPN GUI

Setelah proses instalasi openvpn *client* selesai hal yang perlu dilakukan :

a. Sertifikat yang telah di buatkan di server IPCcop di salin ke computer user di C:\Program File\OpenVPN\Config.
b. Setelah file di salin lalu extrak file tersebut.
c. Double klik openVPN client atau icon openVPN GUI yang telah di install.
d. Maka icon tersebut akan tampil ditray windwos.
e. Klik kanan pada icon yang ada di *tray windows* klik *connect.*
f. Masukkan *password* yang di buat pada server ipcop.
g. Tunggu sampai proses selesai.



Sumber : Hasil Penelitian (2014)

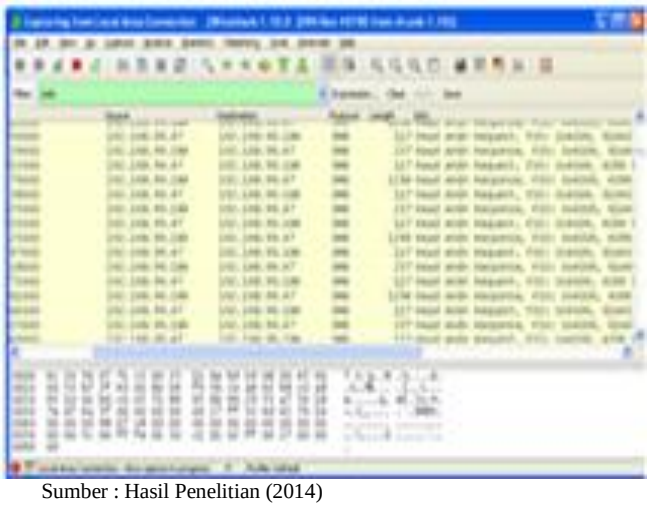
Gambar 14. Gambar Instalasi Selesai

C. Pengujian

Berikut ini akan ditampilkan hasil dari capture paket data dengan menggunakan aplikasi *software* wireshark ketika terjadi lalu-lintas data melalui jaringan tanpa VPN dan jaringan VPN.

1. Pengujian jaringan Awal

Evaluasi Jaringan tanpa VPN ini dilakukan dengan cara melakukan aktifitas tanpa menggunakan koneksi VPN.

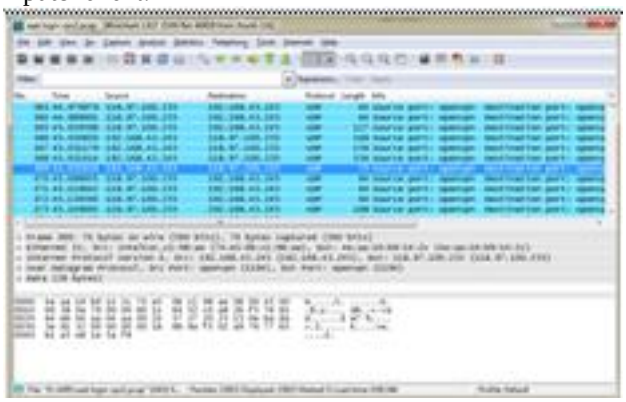


Sumber : Hasil Penelitian (2014)
Gambar 15. Hasil Capture Wireshark Tanpa Menggunakan VPN

Gambar 15. menunjukan hasil dari paket data yang tertangkap dan dilihat isinya adalah bahwa untuk paket data yang dikirimkan tidak ada metode keamanan yang digunakan untuk mengamankan paket data. Dari analisis diatas dapat diketahui performansi dan celah keamanan jaringan pada saat pengiriman data. Dari sekian banyak celah keamanan, *sniffing* merupakan ancaman yang serius. Hal ini dikarenakan kita dapat melihat *username* dan *password* dari suatu sistem agar bisa mengakses masuk ke sistem tersebut.

2. Pengujain Jaringan Akhir

Evaluasi Jaringan dengan VPN ini dilakukan dengan mengaktifkan server VPN dan menjalankan *vpn client* dari komputer *client.*



Sumber : Hasil Penelitian (2014)
Gambar 16. Hasil Capture Wireshark Dengan Menggunakan VPN

Gambar 16 menunjukkan hasil pengujian menggunakan VPN, data yang dikirimkan dari *client* ke *server* tidak dapat dibaca oleh software *wireshark*. Hal ini dikarenakan pada jaringan VPN terdapat metode *tunneling*. Dimana data yang dikirim terenkripsi dan ditambahkan *header* baru sehingga baik data pengirim maupun penerima tidak dapat terlihat.

V. KESIMPULAN

Jaringan komputer sering terjadi adanya gangguan yang mengakibatkan menghambat jalannya kegiatan operasional pada perusahaan yang menggunakannya. Sama seperti yang dialami oleh PT. Kimia Farma Trading & Distribution (KFTD) juga sering mengalami hal yang sama, kendala mengenai kegiatan operasional pada perusahaan yang disebabkan oleh gangguan jaringan komputer dari provider. Jaringan komputer VPN menggunakan OpenVPN IPCop dapat mempermudah pekerjaan user untuk melakukan suatu perkerjaan dimanapun user tersebut berada, selama user dapat menggunakan akses/jaringan data/internet.

REFERENSI

[1] Patih, D. F., Fitriawan, H., & Yuniati, Y. Analisa Perancangan Server VOIP (Voice Internet Protocol) Dengan Opensource Asterisk dan VPN (Virtual Private Network) Sebagai Pengaman Jaringan Antar Client. ISSN : 2303-0577. Lampung : Jurnal Informatika dan Teknik Elektro Terapan , Vol. 1 No. 1 Januari 2012, 42-48.

[2] Aditya, A. Mahir Membuat Jaringan Komputer. Jakarta: Dunia Komputer. 2011.

[3] Micro, A. Dasar-dasar Jaringan Komputer. Banjarbaru. 2012.

[4] Syafrizal, M. Pengantar Jaringan Komputer. Yogyakarta: Andi. 2005.

[5] Wagito. Jaringan Komputer, Teori dan Implementasi Berbasis Linux. Yogyakarta:, Gava Media. 2005.

[6] Winarto, E., Zaki, A., & Community, S. , Membuat Sendiri Jaringan Komputer. Semarang: PT. Elex Media Komputindo. 2013.

[7] Madcom. Sistem Jaringan Komputer untuk Pemula. Madiun: Andi. 2010.

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

PENULIS

Aris Munandar, S. Kom. Tahun 2014 lulus Program Strata Satu di Kampus STMIK Nusa Mandiri dengan Program Studi Teknik Informatika. Saat ini Penulis bekerja di PT.Kimia Farma Trading and Distribution Sebagai untuk Posisi IT.

Mohammad Badrul, M.Kom. Tahun 2009 lulus Program Strata Satu (S1) Program Studi Sistem Informasi di STMIK Nusa Mandiri Jakarta. Tahun 2012 menyelesaikan progarm Srata Dua (S2) di Magister Ilmu Komputer STMIK Nusa Mandiri Jakarta. Selain mengajar, Penulis juga aktif dalam membimbing mahasiswa yang sedang melakukan penelitian khususnya di tingkat Strata 1 dan penulis juga terlibat dalam tim konsorsium di Program Studi Teknik Informatika STMIK Nusa Mandiri untuk penyusunan bahan ajar. Saat ini penulis memiliki Jabatan Fungsional Asisten ahli di kampus STMIK Nusa Mandiri Jakarta. Penulis tertarik dalam bidang kelimuan Data mining, Jaringan komputer, Operating sistem khusunya open source, Database, Software engineering dan Research Metode.