JURNAL TEKNIK KOMPUTER AMIK BSI

IMPLEMENTASI VIRTUAL PRIVATE NETWORK DAN PROXY SERVER MENGGUNAKAN CLEAR OS PADA PT.VALDO INTERNATIONAL

Eka Varianto[1], Mohammad Badrul[2]

Abstract*— A demand for the use of the internet network is perceived by IT workers . Therefore, it is needed once an internet network in a particular company IT division institution , the absence of a private network (VPN) and restrictions on the use of an internet connection can disrupt corporate institutions all parties . to overcome this it will build a server using ClearOS . Open VPN is one of the existing facilities on the ClearOS server that enables IT workers can access the internal office network using a private network connection from outside and Proxy Server with Access Control List Method is a technique selectivity in data communication connection request for a permit or otherwise , number of data packets from a host computer to get to a particular destination . Results of research conducted by the author proves that ClearOS filtering method based Access Control List to filter based on IP addresses identify devices and services as well as the selectivity of query data based on addresses of visited websites.

***Intisari*— Sebuah tuntutan akan penggunaan Jaringan internet sangat dirasakan oleh para pekerja IT. Oleh karena itu sangat dibutuhkan sekali sebuah jaringan internet di sebuah institusi perusahaan khususnya divisi IT, tidak adanya Jaringan pribadi (VPN) dan pembatasan dalam penggunaan koneksi internet suatu institusi perusahaan dapat mengganggu semua pihak. untuk mengatasi hal ini maka akan dibangun sebuah server dengan menggunakan ClearOS. VPN adalah salah satu fasilitas yang ada pada server ClearOS yang memungkinkan para pekerja IT dapat mengakses jaringan internal kantor menggunakan koneksi jaringan pribadi dari luar dan Proxy Server dengan Metode Access Control List merupakan salah satu teknik selektivitas permintaan sambungan dalam komunikasi data untuk mengijinkan atau sebaliknya, sejumlah paket data dari suatu host komputer menuju ke tujuan tertentu. Hasil dari riset yang penulis lakukan membuktikan bahwa ClearOS dengan metode filtering berbasiskan Access Control List dapat menyaring identifikasi perangkat berdasar IP Address dan serta selektivitas permintaan layanan data berdasarkan alamat website yang dikunjungi.**

Kata Kunci: VPN, Proxy Server, ClearOS

[1]Program Studi Teknik Informatika STMIK Nusa Mandiri *Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan. Telp. (021) 78839513 Fax. (021) 78839421*

[2] Sistem Informasi *STMIK Nusa Mandiri Jakarta, Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan. Telp. (021) 78839513 Fax. (021) 78839421, e-mail: eka.varianto@valdo-intl.com; mohammad.mbl@nusamandiri.ac.id*

I. PENDAHULUAN

Jaringan komputer menjadi pilihan yang tepat baik itu perusahaan maupun personal untuk menyediakan informasi dan menghubungkann Jaringan LAN ke internet. Hal ini dapat dilihat dari penggunaan internet yang terus meningkat.

PT. Valdo International adalah perusahaan yang bergerak di bidang *Outsourcing Tele Marketing* bank dan asuransi yang selalu memperhatikan kebutuhan klien akan keamanan data di internet. Ketika klien melakukan pertukaran informasi data, hal ini sangat memungkinkan ada pihak yang melakukan pencurian selama data ditransmisikan di internet.

Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan *Virtual Private Network* (VPN). Teknologi *Virtual Private Network* (VPN) memungkinkan setiap user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada.

Penggunaan VPN (Virtual Private Network) merupakan salah satu alternatif untuk mengirimkan voice, yang bersifat private atau aman, karena penggunaan koneksi yang telah terenkripsi serta penggunaan private keys, certificate, username atau password untuk melakukan authentikasi dalam membangun koneksi[1].

Tidak berbeda jauh dengan VPN, teknologi Proxy Server juga memiliki peranan penting dalam suatu perusahaan baik dalam sekala kecil, menengah dan perusahaan sekala besar. Karena Masalah yang sering muncul di PT. Valdo Internasional adalah ketika user ingin mengakses sebuah alamat web menggunakan internet, user seringkali mengalami kecepatan koneksi atau kecepatan akses lambat dan tidak seperti yang diharapkan. Dikarenakan di PT. Valdo Internasional belum terdapat kontrol jaringan penggunaan koneksi internet di setiap divisi yang menyebabkan bandwidth yang tersedia tidak dapat mencukupi kebutuhan semua user, Masalah seperti ini sering muncul baik di kantor-kantor ataupun di sebuah universitas sekalipun, begitu pun juga yang terjadi di PT. Valdo Internasional yang berlangganan menggunakan salah satu provider internet dengan paket

SOHO yang besaran *Bandwidth*-nya 15 Mbps. Dengan paket tersebut diharapkan dapat mencukupi kebutuhan koneksi internet untuk semua user.

II. KAJIAN LITERATUR

Jaringan komputer adalah sebuah sistem yang terdiri dari atas komputer, *software* dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama [2]. Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta atau menerima layanan disebut pelayan klien (*client*) dan yang memberikan atau mengirim layanan disebut pelayan (server). Arsitektur ini disebut dengan sistem *client server*, dan digunakan pada hamper seluruh aplikasi jaringan komputer.

Jika dilihat berdasarkan luas area yang dapat dijangkau atau dilayani jaringan Komputer terbagi menjadi 3 jenis yaitu LAN, MAN dan WAN.

A. Klasifikasi Jaringan Komputer

1. LAN

LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil [2]. Saat ini, kebanyakaan 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 *Wifi*) juga sering digunakan untuk membentuk LAN dengan teknologi *Wifi* biasa disebut *hotspot*

2. MAN

MAN adalah sebuah jaringan komputer besar yang mencangkup sebuah kota atau sebuah kampus besar[3]. MAN biasanya merupakan gabungan dari LAN yang menggunakan teknologi *backbone* berkecepatan tinggi dan menyediakan layanan ke jaringan yang lebih besar seperti WAN dan *Internet*. *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

3. WAN

Suatu WAN meliputi area geografi yang lebih luas lagi, yang meliput suatu negara atau dunia. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda [3]. 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. *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[2]. 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:

B. Jenis-Jenis Jaringan

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai *client* dan juga *server*. Tetapi ada jaringan yang memiliki komputer yang khusus didedikasikan sebagai *server* sedangkan yang lain sebagai *client*. Ada juga yang tidak memilki komputer yang khusus berfungsi sebagai *server* saja. Karena itu berdasarkan fungsinya maka ada dua jenis jaringan komputer.

1. Client Server

Pada jaringan ini terdapat 1 atau beberapa komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer client[2].

2. Peer to peer

Pada jaringan ini tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua computer berfungsi sebagai *client* sekaligus *server*[2].

C. Perangkat Keras Jaringan

Ada beberapa perangkat keras yang digunakan untuk penelitian ini antara lain:

1. Modem

Modem berasal dari singkatan Modulator Demodulator. Modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan Demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik [4]. Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah.

2. Router

Router sering digunakan untuk menghubungkan beberapa *network*. Baik *network* yang sama maupun berbeda dari sei teknologinya. Router juga digunakan untuk membagi *network* besar menjadi beberapa buah *subnetwork* (*network-network* kecil). Setiap subnetwork seolah-olah "terisolir" dari network lain. Hal ini dapat membagi-bagi *traffic* yang akan berdampak positif pada performa network [2]. Sebuah router memiliki kemampuan routing. Artinya router secara cerdas dapat mengetahui kemana rute perjalanan informasi (yang disebut packet) akan dilewatkan, apakah ditujukan untuk host lain yang satu *network* atau berbeda *network*.

3. Bridge

Bridge atau *transparent bridge* merupakan perangkat network yang digunakan untuk menghubungkan dua buah

LAN (*Local Area Network*) atau membagi sebuah LAN menjadi dua buah segmen. Tujuannya adalah untuk mengurangi *traffic* sedemikian rupa sehingga dapat meningkatkan performa *network* [2].

4. Switch/Hub

Switch adalah *bridge* yang memiliki banyak port, sehingga disebut sebagai *multiport bridge*. *Switch* berfungsi sebagai sentral atau konsestrator pada sebuah network. Switch dapat mempelajari alamat *hardware host* tujuan, sehingga informasi berupa data bisa langsung dikirim ke *host* tujuan [2]. hub mirip dengan *switch*, namun hub tidak secerdas *switch*. Jika *switch* mengirim suatu informasi langsung dikirim ke host tujuan, kalau hub mengirim informasi tersebut kesemua *host*. Kondisi seperti ini menyebabkan beban traffic yang tinggi. Oleh sebab itu, hub biasanya digunakan pada *network* berskala kecil, seperti *network* di Lab.komputer sekolah, warnet dll.

5. Network Interface Card (Nic)

NIC (*network interface card*) adalah expansion board yang digunakan supaya komputer dapat dihubungkan dengan jaringan. sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN *card* (*Local Area Network Card*) [4].

D. ClearOS

ClearOS adalah linux yang di kostumasi khusus untuk keperluan server. Dengan berbagai fitur yang powerfull dan setting yang simple, ClearOS menjadi alternative pilihan, baik untuk pemula yang tidak mengerti linux sama sekali maupun untuk profesional yang memerlukan kemampuan terbaik dari OS linux server. Berbasis Linux Red Hat Enterprise 5, Menjadikan ClearOS memiliki source base yang kuat dan stabil untuk dijalankan sebagai server di warnet, game online, perkantoran, dan perusahaan[4].

E. 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[5] :

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 [5] :

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 [5].

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 [5].

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 [5].

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 [5].

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 [5].

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*[5].

F. VPN

VPN adalah Virtual, karena tidak ada koneksi jaringan langsung nyata antara dua (atau lebih) mitra komunikasi, 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 (tiga) mekanisme penting, yaitu enkripsi, autentikasi dan autorisasi [7].

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 [7]:

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 peneliti menggunakan metode penelitian sebagai berikut :

1. Teknik Pengumpulan Data

   Teknik yang dilakukan untuk pengumpulan data adalah sebagai berikut :

a. Observasi

   Penulis melakukan pengamatan langsung dalam membangun server ClearOS yang akan digunakan sebagai VPN dan Proxy Server di perusahaan tempat penulis melakukan penelitian.

b. Wawancara

   Penulis melakukan proses wawancara dalam membangun server ClearOS dan melakukan tanya jawab terhadap pokok persoalan yang ada dalam penelitian yang penulis ambil.

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

   Penelitian ini menggunakan pemodelan jaringan untuk mensimulasikan sistem VPN Server sebagai Jaringan pribadi di dalam perusahaan dan *filtering* Ip Address yang di fungsikan sebagai Proxy Server untuk melakukan simulasi pemblokiran beberapa situs yang akan menggunakan *ClearOS.* Kebutuhan untuk dibangunnya server ClearOS dengan metode *ACL* guna untuk pemakaian koneksi internet agar dapat menggunakan akses internet sesuai kebutuhan yang diperlukan yang dimana dibutuhkan perangkat lunak dan perangkat keras seperti ClearOS, Putty dan komputer dalam pembuatan server.

b. Desain

   Tahap pertama dalam pembuatan server ClearOS tersebut adalah menginstal ClearOS guna mengaktifkan fitur PPTP VPN Server dan Web Proxy serta *Access Control List* yang berada di ClearOS. Desain yang akan digunakan untuk membangun server ClearOS dan akan diterapkan sebagai VPN dan firewall server dalam keamanan jaringan di PT. Valdo Internasional adalah distro linux ClearOS yang memiliki fasilitas PPTP VPN dan Access Control List (ACL) untuk Proxy Server.

c. Testing

   Untuk tahap testing akan dilakukan di PT. Valdo Internasional yang akan menggunakan Server ClearOS.

VPN Server ClearOS akan bekerja sesuai dengan *User account* yang telah di daftarkan dan *Accesst Control List* berdasarkan IP Address ataupun alamat website yang di daftarkan pada Access Control List (ACL) untuk Proxy Server.

d. Implementasi

Server ClearOS ini akan di implementasikan di PT. Valdo Internasional dimana server ClearOS ini difungsikan sebagai VPN dan Proxy Server yang berfungsi sebagai penghubung jaringan internal dengan menggunakan akses internet dan filter dalam penggunaan internet yang digunakan oleh user setiap hari.

IV. HASIL DAN PEMBAHASAN

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

A. Jaringan yang sedang diterapkan

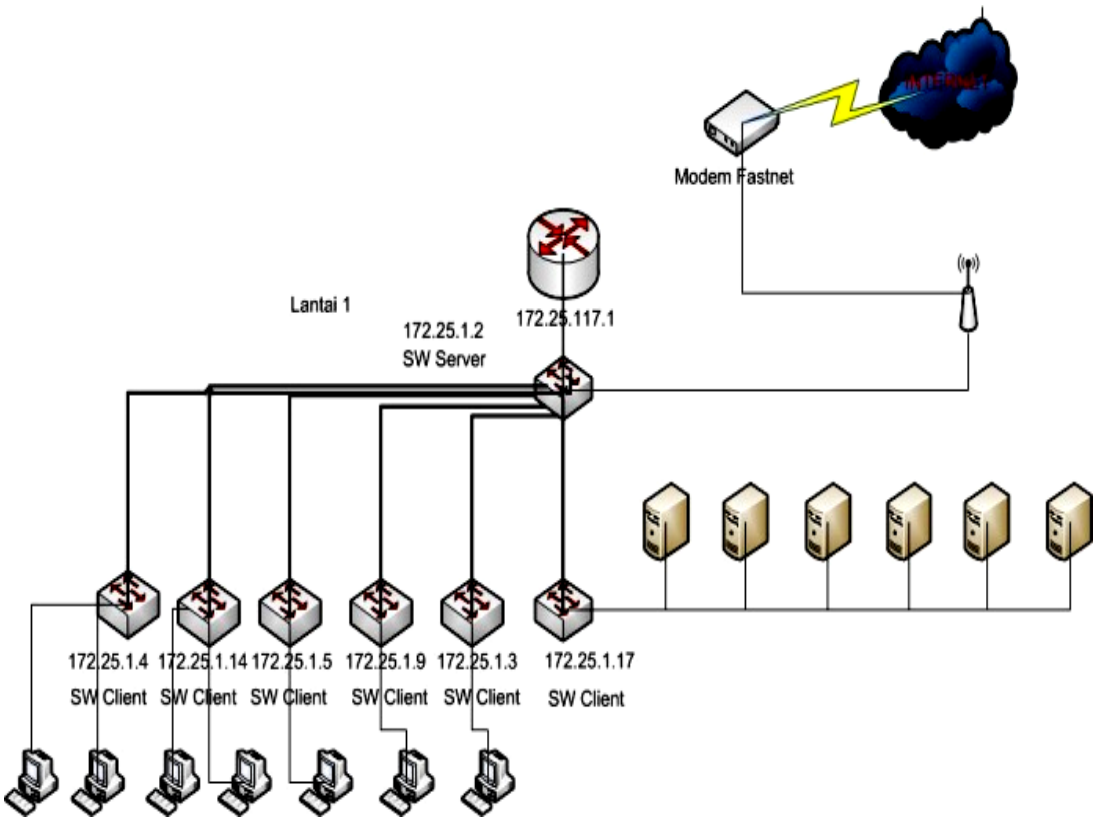
Pembahasan ini penulis akan membahas tentang manajemen jaringan, topologi jaringan, arsitektur jaringan, skema jaringan dan keamanan jaringan.

1. Manajemen Jaringan

Untuk jaringan komputer yang digunakan di PT. Valdo Internasional adalah jenis jaringan LAN (*Local Area Network*), sebuah sistem yang terdiri dari atas komputer, software dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta atau menerima layanan disebut klien (*client*) dan yang memberikan atau mengirim layanan disebut (*server*). Arsitektur ini disebut dengan sistem *client-server* dan digunakan pada hampir seluruh aplikasi jaringan komputer. Untuk penggunaan IP address yang berada di PT. Valdo Internasional menggunakan kelas B dan untuk pengalamatan sendiri menggunakan *network ID* 172.xxx.xxx.xxx, untuk *authentikasi user* sendiri mempunyai hak akses yang berbeda-beda dikarenakan untuk mengakses ke IP yang berbeda harus didaftarkan terlebih dahulu oleh admin *network* ke sebuah perangkat router.

2. Topologi jaringan

Topologi jaringan komputer yang digunakan pada PT. Valdo Internasional adalah topologi *star*, yang mempunyai jaringan komputer yang terdiri dari beberapa buah *switch* dan satu buah *router*. Untuk menghubungkan jaringan komputer di PT. Valdo Internasional, khususnya jaringan yang terpasang pada gedung kantor menggunakan *switch*, dan telah membentuk suatu jaringan komputer LAN.



Sumber : Hasil Penelitian (2014)

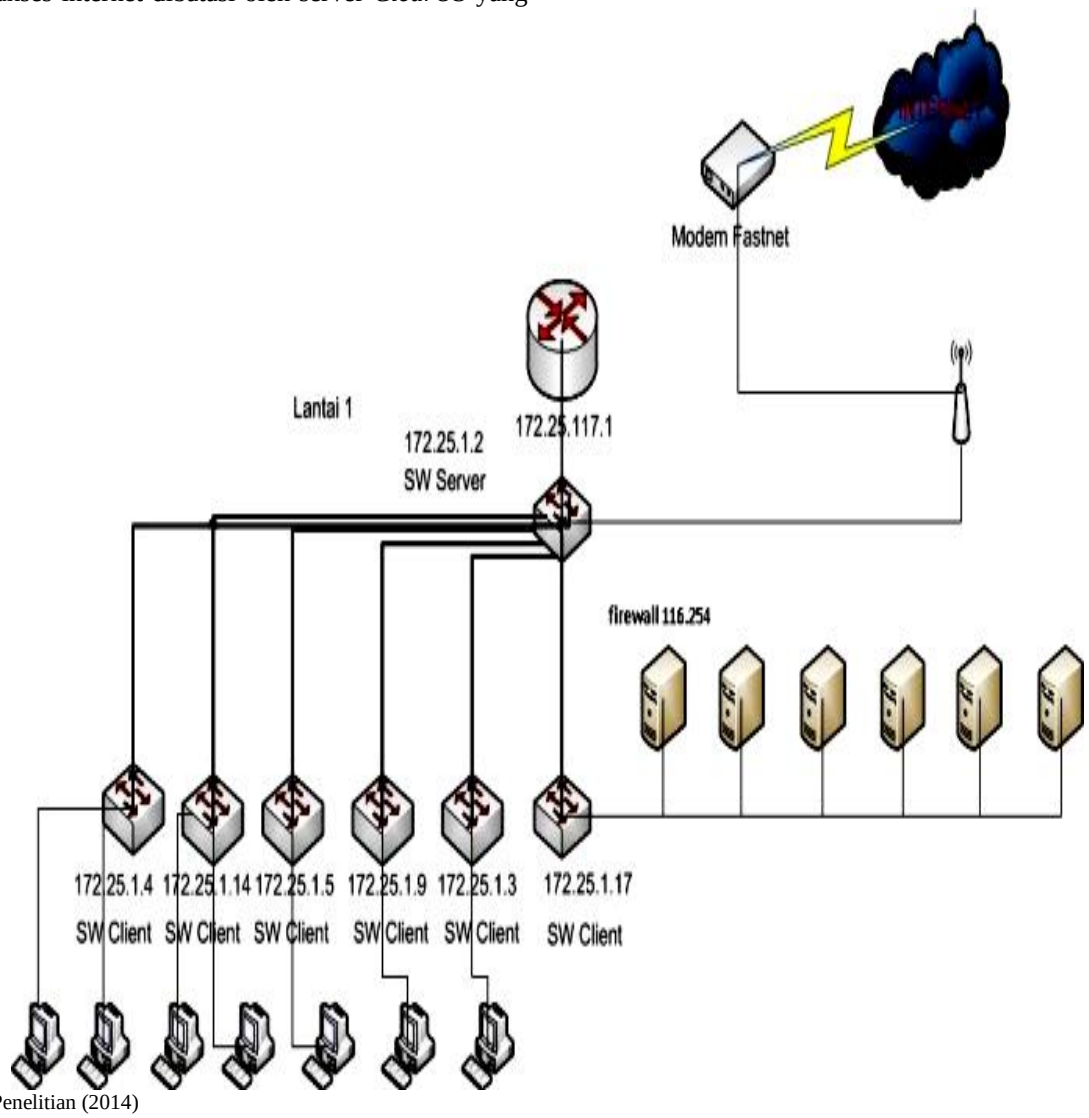
Gambar 1. Topologi Jaringan PT. Valdo

3. Arsitektur Jaringan

Setelah penulis melakukan penelitian di PT. Valdo Internasional ini arsitektur jaringan yang digunakan oleh PT. Valdo Internasional adalah sistem operasi jaringan model LAN (*Local Area Network*). Sistem operasi jaringan LAN memungkinkan user dapat terhubung satu sama lain bila memiliki *host ID* yang sama karena di PT. Valdo Internasional untuk terhubung dengan IP address dan memiliki *host ID* yang berbeda maka IP address tersebut harus didaftar didalam router agar dapat terhubung dengan IP address tujuan. Sedangkan untuk penggunaan koneksi internet tidak semua user dapat menggunakan akses internet secara full akses dikarenakan di dalam PT. Valdo Internasional untuk semua penggunaan akses internet dibatasi oleh server *ClearOS* yang dimana berfungsi sebagai keamanan jaringan. PT. Valdo Internasional juga menggunakan beberapa *Internet Service Provider* (ISP) dalam penggunaan internet maupun mail server. Selain itu penulis mendapatkan beberapa data pengalamatan Ip address jaringan yang terdapat pada PT. Valdo Internasional dan berikut daftar table pengalamatan IP address client dan server di PT. Valdo Internasional.

4. Skema Jaringan

Setelah penulis melakukan riset di PT.Valdo Internasional, penulis dapat menggambarkan topologi bentuk jaringan komputer yang berada di PT. Valdo Internasional. Adapun skema jaringan komputer pada PT. Valdo Internasional yaitu terdapat pada gambar sebagai berikut:



Sumber : Hasil Penelitian (2014)

Gambar 2. Topologi Jaringan PT. Valdo

5. Keamanan Jaringan

Kemamanan jaringan adalah salah satu aspek penting dalam dunia internet suatu jaringan internal perusahaan membutuhkan keamanan khusus yang dapat menjaga data-data penting dari serangan hacker, salah satu caranya adalah memasang *firewall* Untangle.

Cara yang digunakan yaitu menggunakan *packet filtering* di dalam *proxy*, diaplikasikan dengan cara mengatur semua packet IP yang menuju, melewati atau akan dituju oleh packet

tersebut. Pada tipe paket tersebut akan diatur apakah akan diterima dan diteruskan atau di tolak.

Cara kedua menggunakan sistem proxy dimana setiap komunikasi yang terjadi antar kedua jaringan harus dilakukan melalui suatu operator, dalam hal ini proxy server. Beberapa protokol seperti telnet dan SMTP (*Simple Mail Transport Protocol*) akan lebih efektif ditangani dengan evaluasi packet (*packet filtering*), sedangkan yang lain seperti FTP (*File Tranfer Protocol*) dan HTTP (*Hyper Text Transport Protocol*) akan lebih efektif ditangani dengan sistem proxy. Kebanyakan *firewall* menggunakan kombinasi kedua teknik ini (*packet filtering dan proxy*), berikut firewaal yang digunakan di PT. Valdo Internasional.

Sumber : Hasil Penelitian (2014)

Gambar 3. Hasil Print Screen untangle

B. Jaringan Usulan

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

1. Manajemen Jaringan Usulan

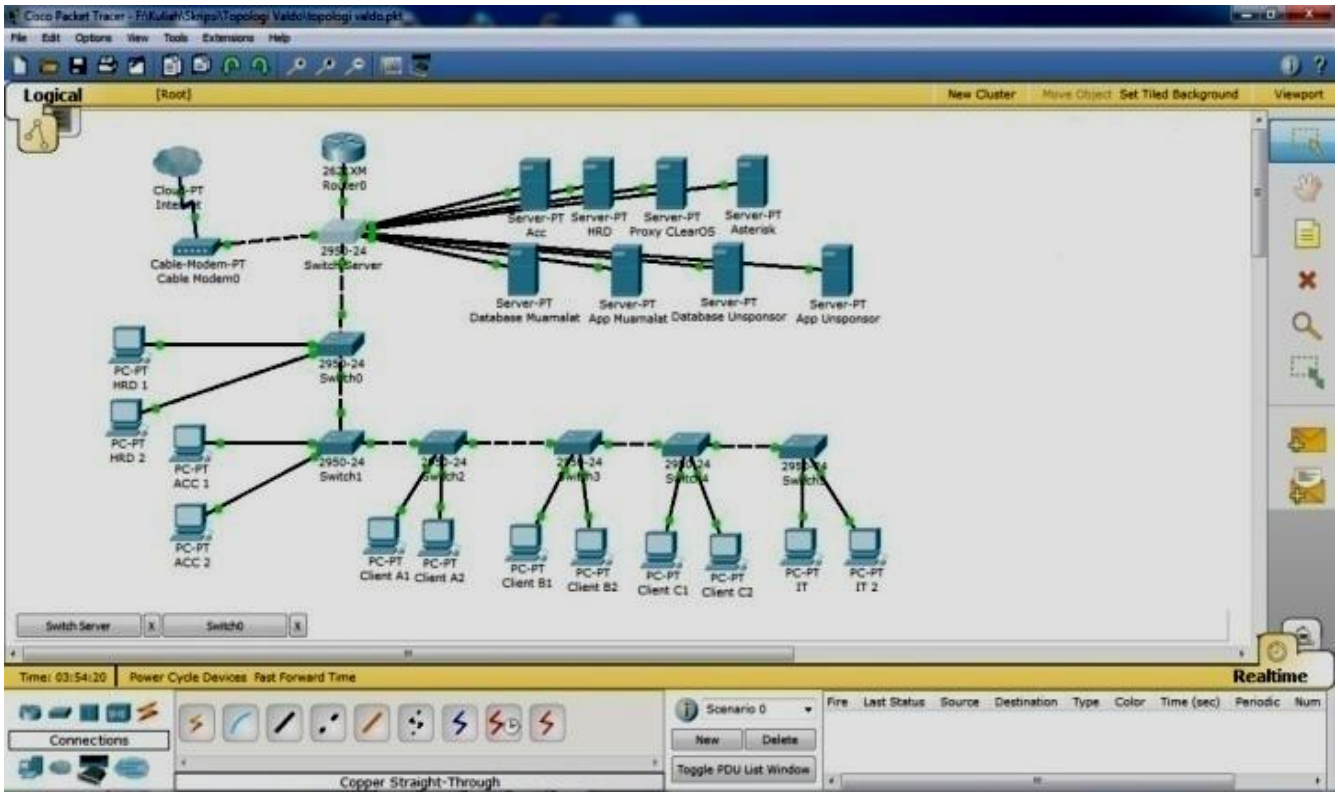
Dalam manajemen jaringan usulan ini penulis mengusulkan untuk lebih optimalisasi keamanan jaringan. Seperti memonitoring jaringan yang sedang berjalan. Dikarenakan jaringan yang berada di dalam PT. Valdo Internasional sudah lumayan besar, maka untuk meningkatkan kinerja jaringan dan penggunaan internet maka dibagun sebuah *server* ClearOS. Hal yang perlu diperhatikan dalam perencanaan pembagunan *server* ClearOS banyaknya *user* yang *online*, kondisi lingkungan jaringan dll.

2. Topologi Jaringan usulan

Penulis mengusulkan untuk menambahkan sebuah *server* ClearOS sebagai keamanan jaringan yang berada di dalam PT. Valdo Internasional untuk membatasi dan memonitoring penggunaan akses internet sedangkan untuk *bandwith* internet yang sudah digunakan untuk koneksi internet sebesar 8Mbps sudah cukup. Dan membutuhkan beberapa perangkat keras untuk membangun sebuah *server* ClearOS sedangkan untuk infrastruktur yang sudah ada didalam PT. Valdo Internasional hanya tinggal dikonfigurasi sedikit untuk melakukan penyesuaian dengan pertumbuhan yang ada.

3. Skema Jaringan Usulan

Pada penelitian ini penulis mencoba untuk menggambarkan usulan penulis dalam bentuk simulasi implementasi jaringan usulan tersebut menggunakan *software simulator*. *Software* yang penulis gunakan adalah Cisco Packet Tracer versi 5.3.2 keluaran dari Cisco, penulis memberikan gambaran koneksi yang digunakan untuk mengimplementasikan jaringan usulan tersebut. Adapun konfigurasi jaringan usulan menggunakan *software simulator* dapat dilihat pada gambar berikut:



Sumber : Hasil Penelitian (2014)

Gambar 4. Skema jaringan usulan kantor pusat

4. Keamanan Jaringan

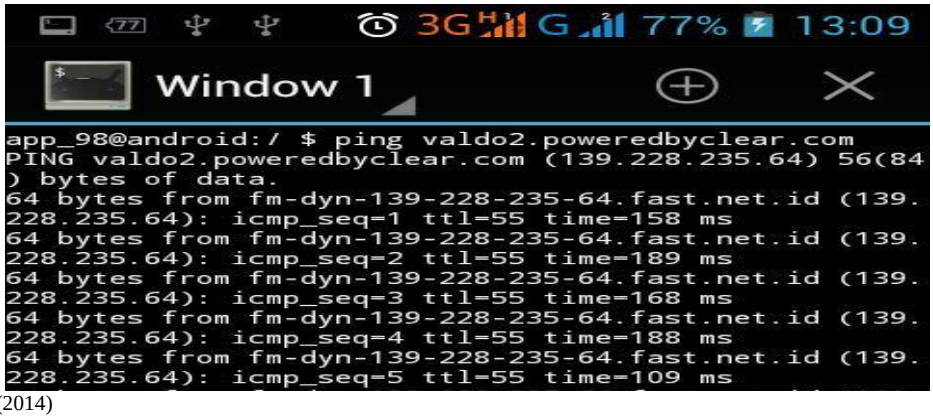
untuk keamanan jaringan yang berada didalam PT. Valdo Internasional penulis mengusulkan untuk menambakan perangkat keras untuk membuat sebuah *server* ClearOS agar penggunaan koneksi internet dapat digunakan secara maksimal. ClearOS merupakan sistem operasi berbasis linux yang ditujukan khusus *server*, *network* dan *gateway*, didesain untuk difungsikan sebagai *All In One server* yang praktis, simple, stabil, dan aman. Dengan ClearOS seorang admin jaringan bisa terhubung dengan melakukan kontrol terhadap sistem kapanpun dan dimanapun berada. Dan didalam server ClearOS ini penulis juga menjelaskan tentang metode PPTP VPN dan *Access Control List* (ACL) pada Proxy server yang penulis ambil sebagai keamanan jaringan.

C. Pengujian

Dalam hal pengujian keamanan jaringan penulis menggunakan pengujian keamanan jaringan menggunakan dua langkah pengujian yaitu:

1. Pengujian jaringan Awal

Pada pengujian keamanan jaringan awal ini penulis mencoba melakukan testing ping ke domain valdo yang digunakan untuk akses VPN dan situs internet sebelum adanya pembatasan koneksi internet dan pendaftaran IP address di server ClearOS.



Sumber : Hasil Penelitian (2014)

Gambar 5. Pengujian Awal ping ke domain VPN

Sumber : Hasil Penelitian (2014)

Gambar 6. Pengujian awal pemakaian internet di PC User

Dari hasil pengujian di atas merupakan hasil pengujian tes ping ke domain VPN PT. Valdo International (Gambar IV.2) dan tes ping ke salah satu website sosial media (Gambar IV.3). User masih dapat menggunakan koneksi internet secara bebas dikarenakan hak aksesnya sebagai pengguna belum dibatasi oleh ClearOS yang berfungsi sebagai *proxy* dan keamanan jaringan.

2. Pengujian Jaringan Akhir

Pada pengujian akhir ini penulis akan mencoba melakukan simulasi konfigurasi PPTP VPN dan konfigurasi Access Control List Proxy Server ClearOS .

a. Mendaftarkan Server ke ClearCenter, ini berfungsi untuk bisa mendapatkan update program terbaru dan mendapatkan Dynamic DNS dari Clear Center secara gratis (ClearCenter / Register)

b.

Sumber : Hasil Penelitian (2014)

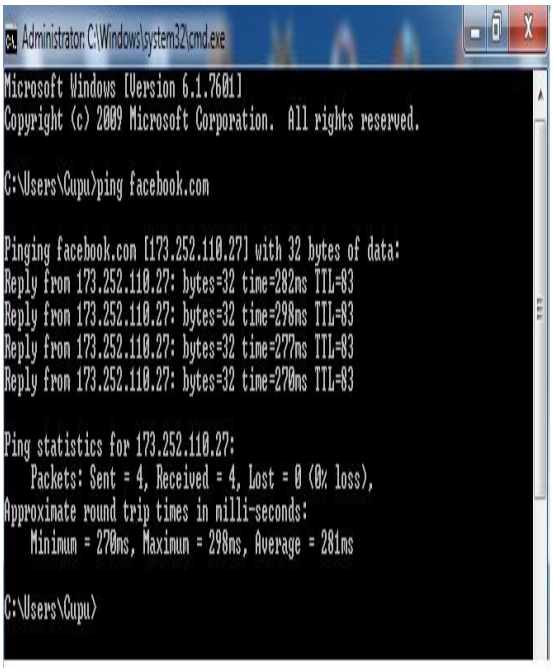
Gambar 7. Pendaftaran Server ke Clear Center

c. Mengaktifkan fitur PPTP VPN (Network / VPN/ PPTP VPN)

Sumber : Hasil Penelitian (2014)

Gambar 8. Konfigurasi PPTP VPN

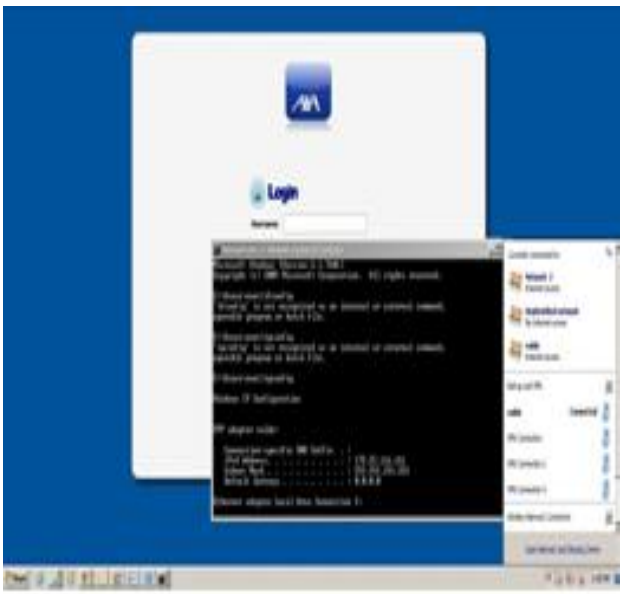
d. Membuat daftar user yang berhak mengakses ke VPN



Sumber : Hasil Penelitian (2014)

Gambar 9. Konfigurasi User untuk mengakses VPN

e. Simulasi Koneksi PPTP VPN dan membuka aplikasi lokal



Sumber : Hasil Penelitian (2014)

Gambar 10. Simulasi koneksi VPN dan mengakses aplikasi local

Dari percobaan koneksi VPN diatas terlihat bahwa koneksi PPTP VPN ke PT. Valdo International sudah berhasil dilakukan dan sudah berhasil mengakses program aplikasi lokal AXA Life insurance. Untuk percobaan ke dua akan disimulasikan pengaktifan fitur Web Proxy dengan menggunakan metode Access List Control (ACL) dalam satu server yang sama. Berikut langkah-langkah yang dilakukan:

a. Masuk ke fiture gateway dan pilih Access Control

Sumber : Hasil Penelitian (2014)

Gambar 11. Pendaftaran IP Address di Menu Access Control

b. Pendaftaran IP Address berdasarkan group divisi

Sumber : Hasil Penelitian (2014)

Gambar 12. Pendaftara IP berdasarkan divisi

c. Tampilan web user yang tidak terdaftar di server ClearOS setelah pengaktifan fitur web proxy

Sumber : Hasil Penelitian (2014)

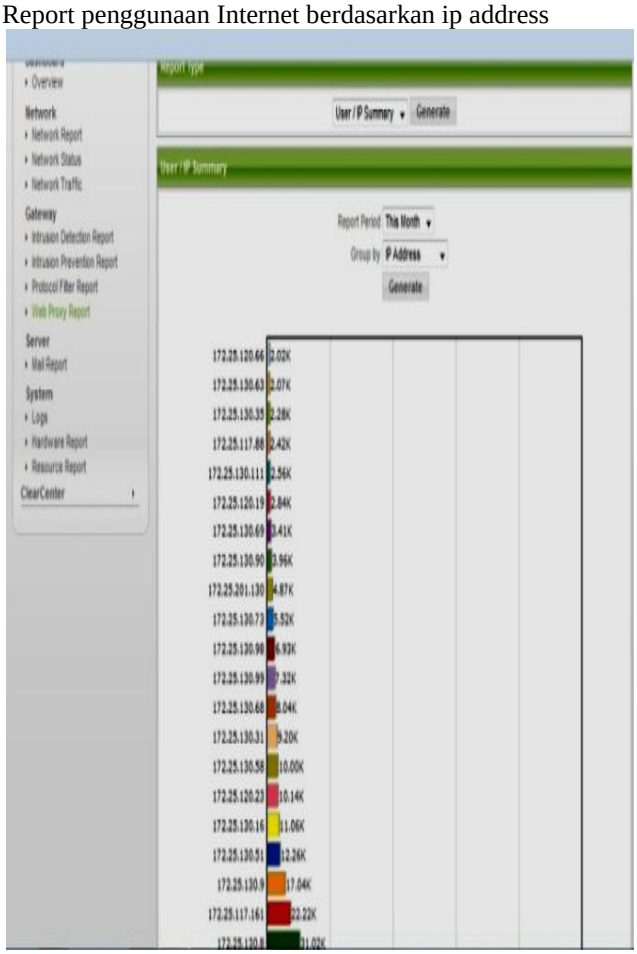
Gambar 13. Ip address yang terkana filter

d. Report penggunaan akses internet harian

Sumber : Hasil Penelitian (2014)

Gambar 14. Report akses internet harian

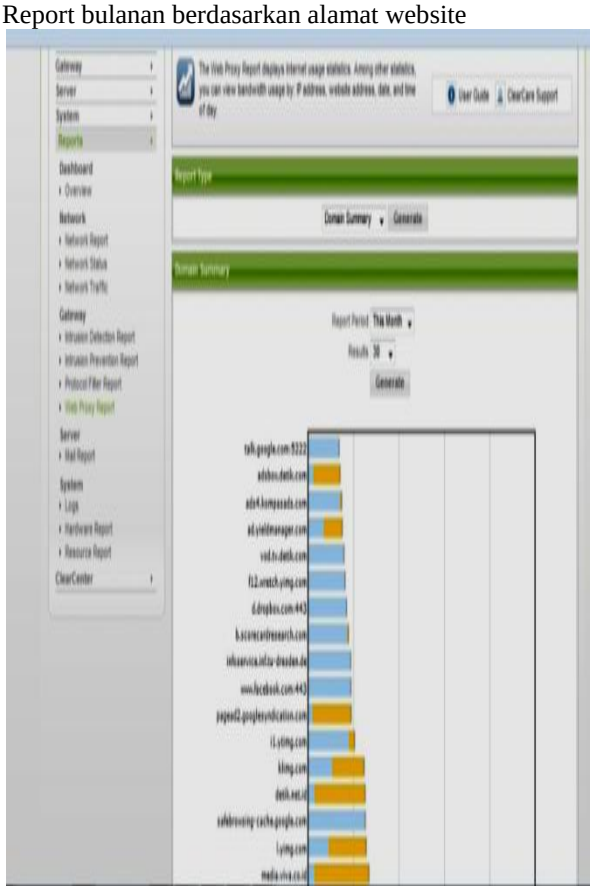
e. Report penggunaan Internet berdasarkan ip address



Sumber : Hasil Penelitian (2014)

Gambar 15. report pengguna intenet berdasarkan ip address

f. Report bulanan berdasarkan alamat website



Sumber : Hasil Penelitian (2014)

Gambar 16. report bulanan berdasarkan alamat website

V. KESIMPULAN

Jaringan komputer sering terjadi adanya gangguan yang mengakibatkan menghambat jalannya kegiatan operasional pada perusahaan yang menggunakannya. Apalagi seperti yang di alami oleh PT. Valdo dimana perusahaan tersebut bergerak dalam bidang jasa IT ke perusahaan yang membutuhkan. Ketika klien melakukan pertukaran informasi data, hal ini sangat memungkinkan ada pihak yang melakukan pencurian selama data ditransmisikan di internet.

Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan Virtual Private Network (VPN). Teknologi Virtual Private Network (VPN memungkinkan setiap user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada.

REFERENSI

[1] Rochim, Adian Fatchur, Andrian Satria Martiyanto. 2011. Desain dan Implementasi Web Proxy danVPN Akses. ISSN: 2087-4685. Semarang: Jurnal Sistem Komputer - Vol. 1 No. 1 Tahun 2011

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

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

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

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

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

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

Eka Varianto, S.Kom. Tahun 2014 lulus dari Program Strata Satu di Kampus STMIK Nusa Mandiri dengan Program Studi Teknik Informatika. Saat ini Penulis bekerja di PT. Valdo International untuk Posisi IT dari tahun 2011 sampai dengan sekarang.

Mohammad Badrul, M.Kom. Tahun 2009 lulus dari Program Strata 1 (S1) STMIK Nusa Mandiri Program Studi Sistem Informasi dan Tahun 2012 lulus dari Program Srata 2 (S2) di STMIK Nusa Mandiri Jakarta dengan Program Studi Ilmu Komputer. 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 Jurusan 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.