Sistem Keamanan Jaringan Komputer Menggunakan Metode NDLC Dengan *Linux Zentyal* Pada Instansi KEMENKO Maritim

Rahmat Yulianto[1], Firdha Aprilyani[2]

Abstract*— The Ministry of Maritime Affairs Coordinating Ministry of government engaged in the implementation of coordination, synchronization, and control of affairs of the Ministry in the administration of government in the maritime field has created a network structure using computer networks as a work support. But in the construction of the network, there was no special server to manage network security, only relying on an Antivirus that functioned as a firewall, this condition was still felt too vulnerable to interference both from inside and outside. Installation of an additional dedicated server as a firewall, VPN, and Filtering IP Table with zentyal operating system that will function as filtering and bandwidth management, with the aim of securing internet access by using a powerful firewall, encrypting file transfers using VPN, blocking potentially hazardous content and manage wireless network security, and provide internet users with safe and fast access. The result is the use of Linux zentyal successfully protects computer networks and functions well in filtering.

Intisari— Kementerian Koordinator Bidang Kemaritiman intansi pemerintah yang bergerak dibidang penyelenggaraan koordinasi, sinkronisasi, dan pengendalian urusan Kementerian dalam penyelenggaraan pemerintahan di bidang kemaritiman telah membuat struktur jaringan dengan menggunakan jaringan komputer sebagai penunjang pekerjaan. Namun dalam pembangunan jaringan tersebut tidak ditemui sebuah Server khusus untuk pengelolaan jaringan Keamanan, hanya mengandalkan sebuah Antivirus yang difungsikan sebagai firewall, kondisi seperti ini dirasa masih terlalu rentan akan gangguan baik yang terjadi dari dalam maupun dari luar. Pemasangan suatu tambahan server dedicated sebagai firewall, VPN, dan Filtering IP Table bersistem operasi zentyal yang akan berfungsi sebagai filtering dan bandwidth management, dengan tujuan untuk mengamankan akses internet dengan menggunakan firewall yang kuat, mengenkripsi transfer file menggunakan VPN , memblokir konten yang berpotensi bahaya dan mengelola kemanan jaringan nirkabel, serta memberikan akses pengguna internet secara aman dan cepat. Hasilnya adalah penggunaan linux zentyal berhasil melakukan perlindungan kepada jaringan komputer dan berfungsi baik dalam melakukan filtering.

Kata Kunci : *Firewall, Filtering, Keamanan Jaringan, zentyal*

[1]*Jurusan Teknik Informatika, STMIK Antar Bangsa, Jl. HOS Cokroaminoto, Kawasan Bisnis CBD Ciledug, Blok A5 No 29-36, Karang Tengah, Tangerang 15157, tlp: 021-50986099; e-mail: rahmat.ryodan@gmail.com*

[2]*Jurusan Sistem Informasi, STMIK Antar Bangsa, Jl. HOS Cokroaminoto, Kawasan Bisnis CBD Ciledug, Blok A5 No 29-36, Karang Tengah, Tangerang 15157, tlp: 021-50986099; e-mail: april.firdha@gmail.com*

I. PENDAHULUAN

Kementerian Koordinator Bidang Kemaritiman adalah instansi pemerintah Yang menjalankan fungsi tugas penyelengara koordinasi, singkronisasi, dan pengendalian urusan Kementerian dalam Pemerintahan di bidang Kemaritiman. Didalam instansi Kementerian Koordinator Bidang Kemaritiman ada 8 (Delapan) bagian untuk membantu Menteri Koordinasi Bidang Kemaritiman yaitu Deputi 1, Deputi 2, Deputi 3, Deputi 4, Biro Umum, Biro Perencanan, Biro Informasi dan Hukum Dan Para Staf Khusus Menteri Koordinasi Bidang Kemaritiman.

Fasilitas jaringan internet sangat dibutuhkan di Kementerian koordinator bidang kemaritiman untuk memaksimalkan kinerja karyawan baik dibidang penyelarasan informasi dan penyimpanan data, agar itu semua dapat terpenuhi maka dibutuhkan jaringan internet yang stabil dan bandwidth yang optimal. Bedasarkan hasil observasi penulis menemukan adanya jaringan internet yang tidak merata, di karenakan karyawan menggunakan layanan konten secara bebas tanpa adanya sistem filtering konten, terdapat kinerja bandwidth yang kurang optimal dan tidak terdapat penyimpanan file di server secara online.

Penulis berharap dengan penggunaan operation system linux Zentyal pada jaringan komputer di Kementerian koordinator bidang kemaritiman dapat menghasilkan traffic jaringan internet yang stabil, memberikan fasilitas kenyamanan pada karyawan Kementerian koordinator bidang kemaritiman dalam menggunakan jaringan secara lokal maupun secara online sehingga karyawan di kementerian koordinator bidang kemaritiman dapat bekerja secara optimal.

Setelah melakukan penelusuran terhadap gambaran jaringan di lapangan, maka dari sekian banyak masalah ditemui mencoba di rumuskan dalam rumusan masalah sebagai berikut :

1. Bagaimana mengelola bandwidth secara optimal pada jaringan keamanan
2. Bagaimana menerapkan sistem filtering pada jaringan keamanan
3. Bagaimana mengembangkan penyimpanan data file melalui via online
4. Bagaimana pemantauan secara traffic melalui monitoring jaringan
5. Bagaimana melindungi atau memblokir konten yang berpotensi bahaya

II. TINJAUAN PUSTAKA

A. Jaringan Keamanan

"Jaringan Komputer adalah hubungan dua buah sampul (umumnya berupa komputer) atau lebih yang tujuan utamanya adalah untuk melakukan pertukaran data''.[1]

B. Jaringan Komputer

"Pengertian keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jarigan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer".[2]

1. Perencanaan Keamanan

Untuk menjamin keamanan dalam jaringan, perlu dilakukan perencanaan keamanan yang matang berdasarkan prosedur dan kebijakan dalam keamanan jaringan. Perencanaan tersebut akan membantu dalam hal-hal berikut ini : [2]

a) Menentukan data atau informasi apa saja yang harus
b) dilindungi.
c) Menentukan berapa besar biaya yang harus ditanamkan
d) dalam melindunginya.
e) Menentukan siapa yang bertanggung jawab
f) untuk menjalankan langkah-langkah yang diperlukan
g) untuk melindungi bagian tersebut.

2. Firewall

Keamanan adalah hal yang penting dalam segala hal. Selayaknya sebuah rumah memiliki pagar, server kita pun membutuhkan 'pagar'. Apalagi server selalu terhubung dengan internet. Isu keamanan sangat penting untuk melindungi server dan data yang tersimpan di dalamnya. 'Pagar' tersebut bernama "firewall" atau "Tembok Api" Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau LAN (local area network). [2]

Firewall mempunyai karakteristik seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan. [2]

Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman. [2]

3. *Virtual Private Network*

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. VPN merupakan koneksi virtual yang bersifat private, dikarenakan jaringan yang dibuat tidak nampak secara fisik hanya berupa jaringan virtual, dan jaringan tersebut tidak semua orang dapat mengaksesnya sehingga sifatnya private. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. [3]

4. Linux Zentyal

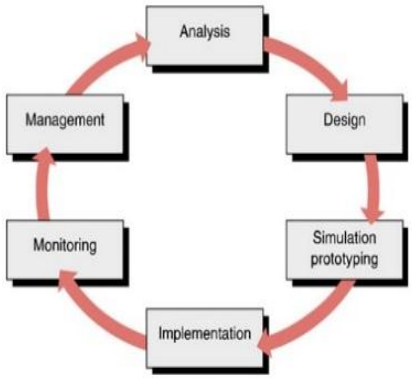
Zentyal adalah Server Linux untuk *Small Business* (UmKM), yang mampu mengelola semua layanan jaringan terpadu dalam satu platform. Zentyal menyediakan Network Gateway, pengelola Infrastruktur, UTM (*Unified Threat Manager*), server untuk perkantoran dan Communications Server. Semua fitur telah terintegrasi dan mudah dikonfigurasi dengan GUI yang membantu administrator hemat waktu. [4]

Sebelumnya zentyal merupakan software opensource (yang dulunya bernama Ebox) untuk Small Business Server, Zentyal dilengkapi dengan webui yang sangat memudahkan untuk mengatur server kita. Dengan webui ini maka user sangat minim sekali setting menggunakan console/terminal.

Seiring perkembangannya zentyal kini hadir sebagai OS sendiri yang dapat didownload, Zentyal OS merupakan turunan dari Ubuntu. Jadi untuk yang sudah familiar dengan ubuntu pasti akan sangat mudah menggunakan zentyal. [4]

III. METODE PENELITIAN

Penelitian dilakukan dengan melakukan riset, dengan metodologi penelitian mengikuti konsep *network development life cycle (NDLC)* [5]



Sumber : [5]

Gbr 1. *network development life cycle* (NDLC)

Adapun penjelasan dari gambar adalah sebagai berikut:

1. Analysis**.**

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya:

a) Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah/operator agar mendapatkan data yang konkrit dan lengkap. Pada kasus di Computer Engineering biasanya juga melakukan brainstorming juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda;
b) Survey langsung kelapangan, pada tahap analisis ju ga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain. Survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan;
c) Membaca manual atau blueprint dokumentasi, pada analysis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut. Begitu juga pada proyek jaringan, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.
d) Menelaah setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap analysis ini adalah :
    1) *User*/*people*: jumlah user, kegiatan yang sering dilakukan, peta politik yang ada, level teknis user;
    2) Media H/W dan S/W: peralatan yang ada, status jaringan, ketersedian data yang dapat diakses dari peralatan, aplikasi S/W yang digunakan;
    3) Data: jumlah pelanggan, jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data;
    4) Network: konfigurasi jaringan, volume trafik jaringan, protokol, *network monitoring* yang ada saat ini, harapan dan rencana pengembangan ke depan;
    5) Perencanaan fisik: masalah listrik, tata letak, ru ang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.

2. *Design*

Dari data-data yang didapatkan sebelumnya, tahap design ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Biasanya hasil dari design berupa :

a) Gambar-gambar topologi (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya);
b) Gambar-gambar detail estimasi kebutuhan yang ada.

3. *Simulation Prototype*.

Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang network seperti *Boson*, *Packet Tracert*, *Netsim*, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan *sharing* dengan *team work* lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para pekerja jaringan yang hanya menggunakan alat bantu tools *Visio* untuk membangun topologi yang akan didesign.

4. *Implementation*.

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pekerja jaringan akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil/gagalnya proyek yang akan dibangun dan ditahap inilah team work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis. Ada beberapa Masalah masalah yang sering muncul pada tahapan ini, diantaranya :

a. Jadwal yang tidak tepat karena faktor-faktor penghambat;
b. Masalah dana/anggaran dan perubahan kebijakan;
c. *Team work* yang tidak solid;
d. Peralatan pendukung dari vendor makanya dibutuhkan manajemen proyek dan manajemen resiko untuk menimalkan sekecil mungkin hambatan-hambatan yang ada.

5. Monitoring.

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada:

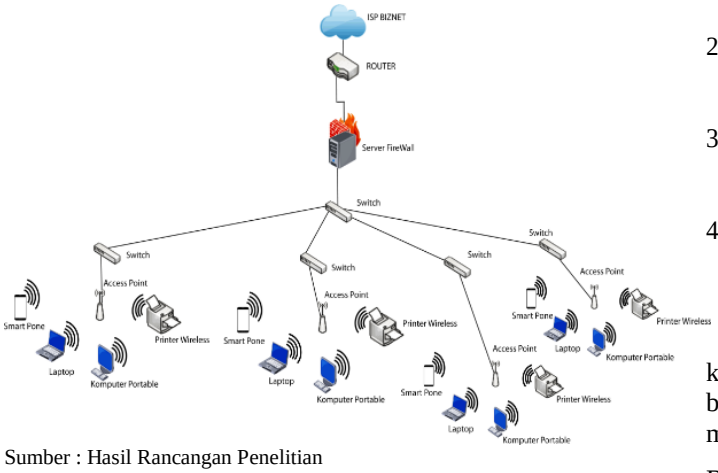
a) Infrastruktur hardware: dengan mengamati kondisi reliability/kehandalan sistem yang telah dibangun (*reliability = performance + availability + security*);
b) Memperhatikan jalannya paket data di jaringan (pewaktuan, *latency*, *peektime*, *troughput*);
c) Metode yang digunakan untuk mengamati kondisi jaringan dan komunikasi secara umum secara terpusat atau tersebar;
d) Pendekatan yang paling sering dilakukan adalah pendekatan Network Management. Dengan pendekatan ini banyak perangkat baik yang lokal dan tersebar dapat dimonitor secara utuh.

6. Management.

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur reliability terjaga. Policy akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan.

IV. HASIL DAN PEMBAHASAN

Pada penelitian ini penulis mencoba untuk menggambarkan usulan penulis dalam bentuk mensimulasikan Jaringan tersebut menggunakan *Software* simulator. *Software* yang digunakan adalah menggunakan VirtualBox 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 Rancangan Penelitian

Gbr 2. Skema Jaringan

Keamanan, kemudahan dan kecepatan transfer (pertukaran data) adalah salah satu aspek yang penting dari suatu jaringan komunikasi, terutama untuk perusahaan-perusahaan skala menengah ke atas. Komunikasi data pada internet melibatkan masalah keamanan, kemudahan dan kecepatan transfer (pertukaran data). Hal ini yang harus diperhatikan oleh pemilik dan administrator sistem informasi suatu perusahaan dalam melakukan kegiatan didunia internet, sehingga kerahasiaan informasi suatu perusahaan bisa terjaga dengan baik dan kemudahan dan kecepatan data (pertukaran data) bisa diimplementasikan sehingga dapat menjadi nilai lebih yang bisa berpengaruh pada cost perusahaan. Untuk karena sebab itu agar karyawan dan para staff dapat saling berkomunikasi khususnya dapat melakukan pekerjaan dari luar lingkungan yang memerlukan koneksi ke dalam jaringan lokal (LAN) Kementerian Koordinator Bidang Kemaritiman Jakarta dengan *internet* yang bersifat *private* yang lebih dikenal dengan *Virtual Privat Network* (VPN). Untuk itu analisa terhadap perangkat jaringan yang akan digunakan dalam perancangan jaringan *private* harus dianalisa dengan cermat untuk meminalisasi permasalahannya.

A. *Firewall*

Zentyal menggunakan subsistem *kernel Linux* disebut *Netfilter* dalam modul *firewall*. Fungsi termasuk penyaringan, paket menandai dan kemampuan koneksi *redirection*. Model keamanan Zentyal didasarkan pada memberikan keamanan maksimum mungkin dengan konfigurasi *default*, berusaha pada saat yang sama untuk meminimalkan upaya saat menambahkan layanan baru.

Ketika Zentyal dikonfigurasi sebagai *firewall*, biasanya dipasang antara jaringan internal dan *router* yang terhubung ke Internet. *Interface* jaringan yang menghubungkan *host* dengan *router* harus ditandai sebagai *Eksternal* di Jaringan *Interfaces*, oleh karena *firewall* dapat menetapkan kebijakan ketat untuk koneksi dimulai di luar jaringan. Bagian dari firewall, tergantung pada arus lalu lintas Setiap salah satu bagian atas adalah yang bertugas mengontrol lalu lintas yang berbeda arus tergantung pada sumber dan tujuan:

1. Penyaringan aturan dari jaringan internal untuk Zentyal (contoh: memungkinkan akses ke Server file Zentyal ini dari jaringan lokal).
2. Aturan penyaringan untuk jaringan internal yang melarang DMZ untuk mengakses segmen LAN lainnya (contoh: membatasi akses ke internet dari satu set host)
3. Aturan penyaringan dari jaringan eksternal untuk Zentyal (contoh: memungkinkan semua host di Internet untuk mengakses halaman web yang dilayani oleh Zentyal).
4. Aturan penyaringan untuk lalu lintas keluar dari Zentyal (contoh: Server koneksi keluar melalui Interface internal / eksternal).

Anda harus mempertimbangkan bahwa memungkinkan koneksi internet untuk layanan Zentyal dapat berpotensi berbahaya, mempelajari implikasi keamanan sebelum memodifikasi set ketiga aturan.

B. *Filtering IP Table*

Iptables merupakan aplikasi untuk administrasi filtering paket dan *Network Address Translation (NAT)* pada IPv4. Gambaran umum, *iptables* digunakan untuk konfigurasi, merawat dan memeriksa rules tables (tabel aturan) tentang *filter* paket IP yang terdapat di kernel linux. Tiap-tiap tables memiliki beberapa built-in (bawaan) chains *kernel linux* dan *chains* buatan *user* sendiri. Setiap chains memiliki *list* / daftar aturan untuk mencocokkan suatu paket yang datang. Setiap aturan tersebut berfungsi memberikan keputusan eksekusi apa yang akan dilakukan bila paket yang datang cocok dengan aturan yang telah dibuat.

Biasanya, setiap aturan memiliki Sumber dan tujuan yang dapat saja, alamat IP atau Obyek dalam kasus lebih dari satu alamat IP atau alamat MAC perlu ditentukan. Di beberapa bagian Sumber atau tujuan dihilangkan karena nilai-nilai mereka sudah dikenal, misalnya Zentyal akan selalu menjadi tujuan dalam aturan penyaringan dari jaringan internal untuk bagian Zentyal dan selalu Sumber dalam aturan penyaringan dari lalu lintas keluar dari Zentyal

Selain itu, setiap aturan selalu dikaitkan dengan Layanan dalam rangka untuk menentukan protokol dan *port* (atau jangkauan port). Layanan dengan *port* sumber yang digunakan untuk aturan yang berkaitan dengan lalu lintas keluar dari layanan internal, misalnya server *HTTP internal*. Sedangkan layanan dengan *port* tujuan yang digunakan untuk aturan yang berkaitan dengan lalu lintas masuk ke layanan internal atau dari keluar lalu lintas ke layanan *eksternal*. Penting untuk dicatat bahwa ada satu set label *generik* yang sangat berguna untuk *firewall* seperti Apa untuk memilih *protokol* atau *port*, atau Apa *TCP*, *UDP* saja untuk memilih protokol *TCP* atau *UDP* masing-masing.

Parameter yang lebih relevan adalah *Keputusan* untuk mengambil sambungan baru. Zentyal memungkinkan parameter ini menggunakan tiga jenis keputusan yang berbeda.

1. Terima sambungan.
2. Deny koneksi, mengabaikan paket yang masuk dan mengatakan sumber yang koneksi tidak dapat dibangun.
3. Mendaftarkan acara koneksi dan terus mengevaluasi sisa aturan.

Dengan cara ini, menggunakan Pemeliharaan *Log -> Log* permintaan *-> Firewall* Anda dapat memeriksa koneksi dicoba. Aturan dimasukkan ke dalam tabel di mana mereka dievaluasi dari atas ke bawah. Setelah (Menyangkal / Menerima) aturan cocok sambungan, keputusan diambil dan penyaringan berhenti, sehingga aturan di bawahnya tidak dianggap. Aturan penebangan menghasilkan log dan terus mengevaluasi aturan. Sebuah aturan generik pada awal rantai dapat memiliki efek mengabaikan yang lebih spesifik yang terletak di kemudian daftar, ini adalah mengapa urutan aturan adalah penting. Anda juga dapat menerapkan logis untuk tidak evaluasi aturan menggunakan pertandingan *Inverse* untuk menentukan kebijakan yang lebih maju.

C. *Virtiual Private Network (VPN)*

Zentyal dapat dikonfigurasi untuk mendukung klien jarak jauh Ini berarti *server* Zentyal bertindak sebagai *gateway* dan *server VPN*, dengan beberapa jaringan area lokal *(LAN)* di balik itu, memungkinkan klien eksternal untuk terhubung ke jaringan lokal melalui layanan *VPN*.

Tujuannya adalah untuk menghubungkan *server* data dengan 2 klien lain jarak jauh dan juga klien jarak jauh satu sama lain. Pertama, Anda perlu membuat Otoritas Sertifikasi dan sertifikat individu untuk dua remote klien. perlu secara eksplisit membuat sertifikat yang unik untuk setiap pengguna yang akan terhubung ke *VPN* melalui *General Authority* Sertifikasi Perhatikan bahwa Anda juga membutuhkan sertifikat untuk *server VPN*. Namun, Zentyal akan membuat sertifikat ini secara otomatis. Dalam skenario ini, Zentyal bertindak sebagai Otoritas Sertifikasi**.**

Alamat *VPN* Menunjukkan *subnet virtual* di mana *server VPN* akan berlokasi dan klien memiliki. Anda harus berhati-hati bahwa jaringan ini tidak tumpang tindih dengan yang lain dan untuk tujuan firewall, itu adalah jaringan internal. Secara *default* 192.168.160.1/24, klien akan mendapatkan alamat 0,2, *. 3 *, Server sertifikat, Sertifikat yang akan menunjukkan server ke klien. *The Zentyal CA* masalah dengan bawaan sertifikat untuk server, dengan nama *vpn-<yourvpnname>*. Kecuali jika ingin mengimpor sertifikat *eksternal*, biasanya akan mempertahankan konfigurasi ini.

Otorisasi klien dengan nama umum: Membutuhkan bahwa nama umum dari sertifikat klien akan mulai dengan *string* yang dipilih dari karakter untuk mengotorisasi koneksi. *Interface TUN* Secara *default Interface* tipe *TAP* digunakan, lebih mirip dengan sebuah jembatan *Layer 2*. Juga dapat menggunakan *Interface* tipe *TUN* lebih mirip dengan node *IP Layer* 3.

Network Address Translation Disarankan untuk mengaktifkan terjemahan ini jika *server* Zentyal yang menerima koneksi *VPN* tidak *default gateway* dari jaringan internal untuk yang dapat mengakses dari *VPN*. Seperti ini klien jaringan *internal* yang ini menanggapi *Zentyal VPN* bukan gateway. Dikareanakan *server Zentyal* adalah kedua dari *server VPN* dan *gateway*.

D. Rancangan Aplikasi

Dalam perancangan sistem jaringan VPN dan FTP yang berada di gedung Kementerian Koordiantor Bidang Kemaritiman Jakarta ini penyusun melakukan konfigurasi terhadap komputer *server* yaitu VPN *server* dan FTP *server* yang berfungsi untuk melayani permintaan dari client untuk bisa terhubung kedalam jaringan *local* komputer di Kemenko, sehingga dapat melakukan proses transfer data dan lain sebagainya. Selain itu penulis juga melakukan proses konfigurasi pada komputer client, sehingga bisa terhubung ke VPN server dan FTP server di jaringan local SETJEN.

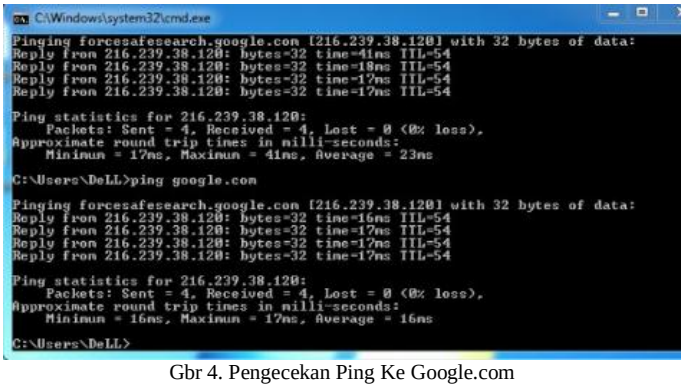
E. Pengujian Jaringan

Pada tahap ini penulis melakukan uji coba terhadap jaringan komputer pada instansi Kemenko Maritim. Hal ini perlu dilakukan karena pengujian ini dilakukan untuk mengetahui apakah keamanan jaringan komputer Instansi Kemenko Maritim sudah berjalan dengan optimal seperti yang diharapkan.

1) Pengujian Jaringan Awal
   a) Pengecekan koneksi internet pada komputer user pada jaringan *zentyal server*.

Gbr 3. Pengecekan Koneksi Internet

   b) Ping dari komputer user ke arah google.com



Gbr 4. Pengecekan Ping Ke Google.com

c) Pengcekan kecepatan transfer data pada jaringan kemenko maritim dengan mengunakan speedtest.

Gbr 5. Pengecekan transfer data

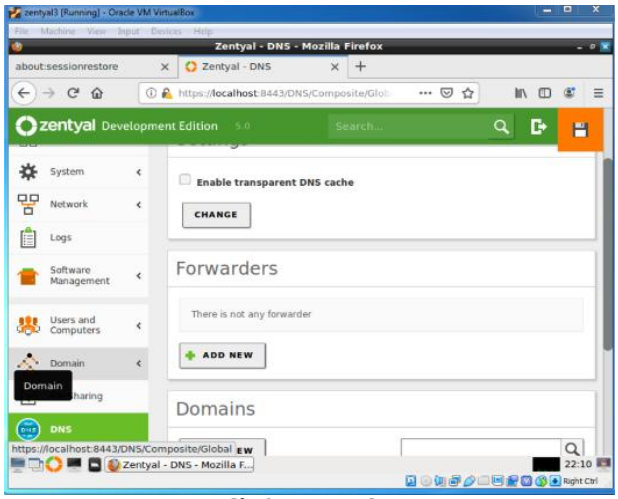
d) Pengecekan web konten yang belum terblokir terlihat disini www.facebook.com masih terbuka sehingga dapat mengurangi kinerja karyawan.

Gbr 6. Web www.facebook.com

2) Pengujian Jaringan Akhir

Layar login ini meminta *username* dan *password* pengguna administrator yang dibuat selama instalasi Oprasi Sistem, untuk kofigurasi sistem jaringan keamanan komputer

Gbr 7. Layar Login

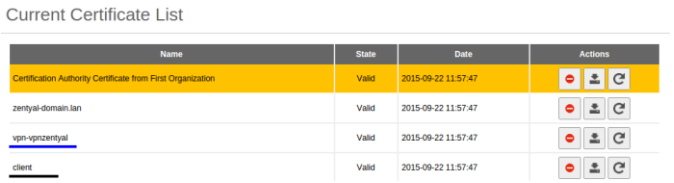


Gbr 8.Layar DNS

a) Alamat IP dibawah ini merupakan alamat yang di pergunakan untuk pengguna user pada server zentyal. Administrator dapat filtering IP tersebut bila penggunaan *bandwith* pada IP Tersebut melampaui batas

Gbr 9. Layar IP table

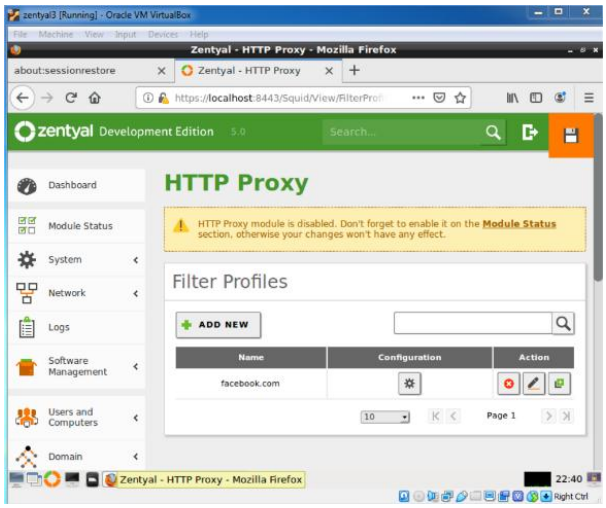
b) Konfigurasi VPN pada *server zentyal*



Gbr 10. Konfigurasi *VPN Zentyal*

Server sertifikat (garis bawah biru) dan sertifikat klien (garis bawah hitam) Setelah Anda memiliki sertifikat, kemudian mengkonfigurasi *server VPN Zentyal* dengan memilih Buat *server* baru. Satu-satunya nilai yang Anda perlu memasukkan untuk membuat *server* baru nama. Zentyal memastikan tugas menciptakan *server* VPN mudah dan menetapkan nilai konfigurasiotomatis

c) Filtering Web Konten Pada Facebook yang penempatan pada HTTP Proxy

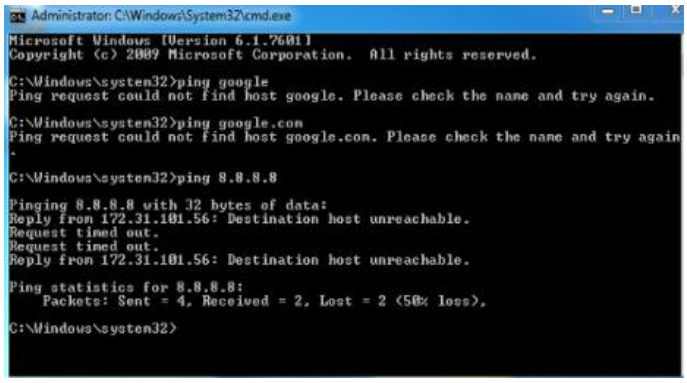


Gbr 11. Konfigurasi *filtering* Web Konten

d) Hasil *filtering* Ip table pada user yang pengunaan *bandwith* Melebihi kapasitas terlihat komputer user berada pada jaringan zentyal dan tidak dapat menggunakan Hak akses internet.

Gbr 12. *No Internet Access*

e) Pengecekan koneksi internet dengen penggunaan ping dari komputer user ke arah google.com setelah konfigurasi filtering IP table. Terlihat pada gambar tersebut terjadi adanya *RTO (Request Timed out).*

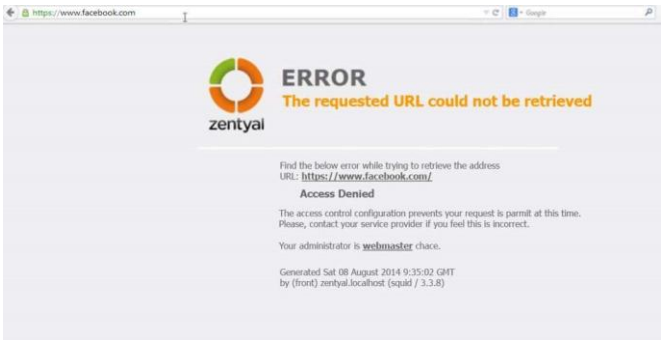


Gbr 13. *Ping RTO*

f) Hasil *Speedtest bandwith* setelah konfigurasi vpn pada linux zentyal server terlihat *bandwith* lebih lambat di bandingkan sebelum menggunakan VPN pada linux *Zentyal*. Dikarenakan *ekripsi* pada *transfer* data tersebut berjalan dengan baik.

Gbr 14. Hasil *Speedtest VPN*

g) Gambar dibawah merupakan hasil *filtering web* konten *facebook* yang di ingin di akses oleh *user*.



Gbr 15. Hasil *Filtering web* konten *facebook.com*

V. PENUTUP

Setelah melakukan pengamatan dan analisa serta melakukan percobaan terhadap linux zentyal yang digunakan sebagai firewall pada jaringan Kementerian Koordinator Bidang Kemaritiman maka didapat kesimpulan sebagai berikut :

1. Linux Zentyal dapat digunakan sebagai gateway dan firewall yang kuat murah serta handal
2. Linux zentyal dapat mengoptimalkan bandwidth management.
3. Linux Zentyal dapat digunakan Memblokir dan memfilter konten yang berpotensi bahaya.
4. Linux Zentyal dapat memberikan akses pengambilan data secara aman dan cepat ketika berada di luar kantor.

REFERENSI

[1] Kristanto, Andri. Keamanan Data Pada Jaringan Komputer. Yogyakarta: Gava Media. 2005.
[2] Wagito. Jaringan Komputer. Jakarta: Gava Media. 2007.
[3] Prihatin Oktivasari, Andri Budhi Utomo, "Analisa Virtual Private Network Menggunakan OpenVPN dan Point to Point Tunneling

Protocol", Jurnal Penelitian Komunikasi dan Opini Publik Vol. 20, No.2, 2016.
[4] Exekias. Zentyal As A Gateway: The Perfect Setup. Diambil dari: http://www.howtoforge.com/zentyal-as-a-gateway-the-perfect-setup (25 februari 2015). 2011
[5] Jaelani, A., 2014. Metode - Metode dalam Metodologi Peneitian. [Online] Available at: https://sites.google.com/a/student.unsika.ac.id/metodepenelitianowl/Tugas-updates/metode-metode dalammetodologipeneitian [Accessed 21 October 2015].

Rahamat Yulianto. Lahir di Tangerang pada Tanggal 09 Juli 2019. Tahun 2019 lulus dari Program Strata Satu (S1) Jurusan Teknik Informatika di STMIK Antar Bangsa. Bekerja pada Kemnterian Koordinator Bidang Kemaritiman Dan Investasi.

Firdha Aprilyani. Lahir di Tangerang pada Tanggal 20 April 1993. Lulus dari Program Strata Satu (S1) Jurusan Sistem Informasi di STMIK Antar Bangsa pada Tahun 2015. Lulus dari Program Pasca Sarjana (S2) Teknologi Sistem Informasi, Universitas Budi Luhur Konsentrasi Teknologi Sistem Informasi pada tahun 2018. Saat ini aktif sebagai Dosen Tetap di STMIK Antar Bangsa, aktif sebagai peneliti dan penulis jurnal ilmiah, serta aktif sebagai anggota Asosiasi Perguruan Tinggi Ilmu Komputer (APTIKOM) dan Asosiasi Dosen Indonesia (ADI) .