LAPORAN KERJA PRAKTEK

Perancangan Firewall Sebagai Security dan Infrastruktur Pada Hotel Alila Villas Uluwatu

Studi dibuat untuk memenuhi salah satu syarat dalam menyelesaikan
Program Strata Satu pada Jurusan Teknik Informatika Fakultas Ilmu Komputer
Universitas Esa Unggul

Disusun oleh :

Nur Ramdhani Siswanto (2008 81 116)

JURUSAN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS ESA UNGGUL

JAKARTA

2012

LEMBAR PENGESAHAN

Laporan Kerja Praktek

Dengan Judul :

Perancangan Firewall Sebagai Security dan Infrastruktur Pada Hotel Alila Villas Uluwatu

Diajukan Untuk Memenuhi

Persyaratan Kurikulum Sarjana Strata-1

Jurusan Teknik Informatika

Universitas Esa Unggul

Disusun Oleh

Nama : Nur Ramdhani Siswanto

NIM : 2008-81-116

Telah Diketahui dan Disetujui Oleh:

(Ir. I Joko Dewanto, MM)	**(Yan Martin)**
Pembimbing Materi	**Pembimbing Lapangan**

(Fransiskus Adikara,S.Kom.,M.Kom)

Koordinator Kerja Praktek

KATA PENGANTAR

Puji syukur kehadirat Allah SWT Yang Maha Mendengar lagi Maha Melihat dan atas segala limpahan rahmat, taufik, serta hidayah-Nya sehingga penulis dapat menyelesaikan laporan kerja praktek yang berjudul "Perancangan Firewall Sebagai Security dan Infrastruktur Pada Hotel Alila Villas Uluwatu" ini sesuai dengan waktu yang telah direncanakan.

Shalawat serta salam semoga senantiasa tercurahkan kepada baginda Nabi Besar Muhammad SAW beserta seluruh keluarga dan sahabatnya yang selalu eksis membantu perjuangan beliau dalam menegakkan Dinullah di muka bumi ini.

Penyusunan laporan kerja praktek ini adalah merupakan salah satu syarat untuk memperoleh gelar sarjana pada Fakultas Ilmu Komputer Jurusan Teknik Informatika di Universitas Esa Unggul

Dalam penulisan laporan kerja praktek ini, tentunya banyak pihak yang telah memberikan bantuan baik moril maupun materil. Oleh karena itu penulis ingin menyampaikan ucapan terimakasih yang tiada hingganya kepada :

1. Bapak Ari Pambudi,S.Kom.,M.Kom selaku dekan fakultas ilmu komputer
2. Bapak Fransiskus Adikara,S.Kom.,M.Kom selaku Kajur jurusan teknik informatika
3. Bapak Ir.I Joko Dewanto selaku pembimbing materi
4. Delon Alfred Gultom selaku *network engineer* yang telah membantu penulis mengumpulkan data dan memberika arahan.
5. Secara khusus penulis ingin mengucapkan kepada Kakak-kakak ku yang selama ini terus mendukung, Ayahanda, serta Alm.Ibuku, sehingga penulis dapat menyelesaikan studi dengan baik.

6. Ucapan terima kasih penulis kepada semua sahabat yang telah banyak memberikan bantuan, dorongan, serta motivasi sehingga laporan kerja praktek ini dapat terselesaikan

Penulis menyadari bahwa laporan kerja praktek ini masih jauh dari kesempurnaan , maka saran dan kritik yang konstruktif dari semua pihak sangat diharapkan demi penyempurnaan selanjutnya.

Akhirnya hanya kepada Allah SWT kita kembalikan semua urusan dan semoga laporan kerja praktek ini dapat bermanfaat bagi semua pihak, khususnya bagi penulis dan para pembaca pada umumnya, semoga Allah SWT meridhoi dan dicatat sebagai ibadah disisi-Nya, amin

Jakarta Februari 2012

(Nur Ramdhani Siswanto)

NIM : 2008-81-116

ABSTRAK

Perancangan ini bermula dari nol, dimana internet baru pertama masuk, sehingga penulis mencoba memberikan rancangan, agar keinginan Alila Uluwatu yang dapat memonitoring lalu lintas jaringannya dapat terwujud. Dimana Alila Uluwatu juga berkeinginan membangun jaringan akses pribadi yang aman. Untuk itu penulis mencoba memberikan rancangan menggunakan *Cisco Asa* 5510 yang bertindak sebagai *firewall* atau *security* jaringan. Tujuan dari pembuatan laporan yang berjudul "Perancangan Firewall Sebagai Security dan Infrastruktur Pada Hotel Alila Villas Uluwatu" ini adalah untuk memberikan rancangan topologi jaringan kepada Alila hotel agar rencana pembangunan jaringan tersebut dapat berjalan. Alila Uluwatu belum memiliki jaringan, topologi ini akan menjadi rancangan awal dalam melakukan pembangunan jaringan tersebut. Metodologi dari peracangan ini adalah, *waterfall* yang terdiri dari *system engineering, analysis,* dan *design*. Karena hanya penulisan ini hanya perancangan, sehingga metodologi yang digunakan hanya sampai *design.*

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR ISI

HALAMAN

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Dunia maya atau yang lebih kita kenal dengan *internet* merupakan dunia tanpa batas, segala hal apapun bisa kita cari dan dapatkan disana, tidak seperti jaman dahulu, *internet* yang masih sangat langka atau bisa dibilang adalah suatu barang mahal, namun sekarang *internet* bukan lagi barang mahal atau langka, sudah setiap orang bisa mendapatkan dengan mudah. Di dalam dunia tanpa batas tersebut bukan hanya hal positif yang bisa kita dapatkan, hal negatif juga bisa kita dapatkan tanpa sengaja, seperti *virus, malware, phising, sniffing*. Untuk itu, bagi para perusahaan besar atau menengah, bahkan perusahaan kecil, berusaha melindungi jaringan mereka masing-masing.

Alila Villas Uluwatu berencana membangun jaringan *LAN* yang berfungsi sebagai fasilitas internet bagi para tamunya, dimana setiap tamu bisa menikmati internet secara gratis. Namun jaringan tersebut juga berfungsi sebagai sarana kontrol oleh perusahaan utama, dimana perusahaan utama dapat memantau keadaan jaringan yang ada disana, selain itu Alila ingin merancang suatu akses jarak jauh yang sangat aman, dimana tidak sembarangan orang dapat masuk, hanya orang yang dipilih, dalam hal ini si *network engineer* dan pemimpin hotel tentunya.

Alila akan menggunakan *Cisco Asa* 5510 sebagai pilihannya. *Cisco Asa* 5510 merupakan *firewall* jaringan. Alat tersebut dapat mewujudkan rencana pembangunan jaringan *LAN* dan sebagai kemananan jaringan.

1.2. Identifikasi Masalah

Berdasarkan latar belakang, penulis mengidentifikasikan masalah yang ditemukan, yaitu sebagai berikut :

1.2.1. Bagaimana merancang jaringan hotel Alila Villas Uluwatu yang handal dari sisi keamanan ?

1.3. Tujuan Penulisan

Tujuan dari penulisan ini adalah sebagai berikut,

1.3.1. Memaparkan hasil rancangan topologi jaringan pada hotel Alila Villas Uluwatu.

1.4. Manfaat Penulisan.

Manfaat dari penulisan ini adalah,

1.4.1. Memaparkan suatu topologi, dan mengenalkan apa itu topologi jaringan.

1.4.2. Menjelaskan bagaimana melindungi suatu jaringan dan mengapa jaringan layak mendapatkan perlindungan.

1.5. Ruang Lingkup Masalah

Penyusunan laporan kerja praktik ini adalah mengenai rancangan topologi jaringan hotel Alila Villas Uluwatu. Dibatasi hanya perancangan menggunakan *Cisco Asa* 5510 yang bertindak sebagai *firewall* sehingga Alilla Uluwatu dapat membangun suatu jaringan yang dapat dikelola oleh perusahaan dan dapat membangun suatu jaringan akses pribadi.

1.6. Sistematika Penulisan

Dalam sistematika penulisan kerja praktek akan menguraikan secara umum setiap bab untuk mendapatkan gambaran singkat mengenai kerja praktek ini, dengan mengikuti urutan penyajian sebagai berikut :

BAB 1 PENDAHULUAN

Pada bab ini penulis membahas tentang latar belakang, perumusan masalah, tujuan, manfaat, ruang lingkup, dan sistematika,

sebagai langkah awal dari penyusunan kerja praktek ini.

BAB 2 LANDASAN TEORI

Pada bab ini penulis membahas tentang teori-teori dasar, tinjauan pustaka, dan model yang berhubungan dengan penulisan kerja praktek ini.

BAB 3 GAMBARAN UMUM PERUSAHAAN

Pada bab ini penulis akan membahas tentang gambaran perusahaan dari Alila Villas Uluwatu, visi dan misi, struktur organisasi, serta metodologi penelitian yang digunakan penulis.

BAB 4 PEMBAHASAN

Pada bab ini penulis akan menjelaskan topologi rancangan yang diberikan kepada Alila Villas Uluwatu, serta proses kerja dari topologi tersebut.

BAB 5 KESIMPULAN dan SARAN

Pada bab ini penulis akan mengemukakan kesimpulan dan saran terhadap perusahaan tersebut. Kesimpulan diperoleh berdasarkan saat pengerjaan perancangan topologi.

BAB 2
LANDASAN TEORI

2.1 **Perancangan**

Perancangan adalah aktifitas kreatif menuju suatu yang baru dan berguna yang tidak ada sebelumnya. Perancangan dapat juga diartikan menuangkan ide atau kreasi dengan memikirkan sesuatu yang pernah ada dan memodifikasinya kemudian menuangkannya kedalam bentuk yang baru.

Sementara dalam Kamus Besar Bahasa Indonesia, definisi perancangan yang berasal dari kata dasar rancang adalah sebagai berikut: "Perancangan atau rancang adalah proses, cara, pembuatan merancang."

Perancangan Sistem Menurut Burch, dikutip oleh Jogiyanto H.M (1993:20) memaparkan "Perancangan sistem sebagai penggambaran, perencanaan, dan pembuatan sketsa/pengaturan atas beberapa elemen yang terpisah ke dalam suatu kesatuan yang utuh dan berfungsi" Sedangkan menurut Scott, dikutip oleh Jogiyanto H.M (1993:23) memberikan definisi bahwa "Rancangan sistem adalah kegiatan untuk menentukan bagaimana suatu sistem akan menyelesaikan apa yang harus diselesaikan, tahap ini menyangkut mengkonfigurasikan komponen komponen perangkat lunak dan perangkat keras suatu sistem sehingga setelah instalasi atas sistem akan benar-benar memuaskan rancang bangun yang telah ditetapkan pada akhir tahap analisis sistem.

Perancangan jaringan adalah proses yang *mystic-mixture art*, *science*, keberuntungan (*luck*) dan terjadi begitu saja (*accident*). Meskipun penuh dengan proses yang misterius ada banyak jalan dan strategi untuk melaluinya.

(1)Jumlah *node* dan pendelegasian tugas. Isu yang banyak dikenal dalam perancangan jaringan adalah jumlah *node*/titik yang ada. Dari

jumlah *node* yang ada bisa kita definisikan tugas yang harus dikerjakan oleh setiap *node*, misalnya karena jumlah *node* sedikit *print-server* cukup satu disambungkan di server atau di salah satu *workstation*. Jika jumlah *node* lebih banyak ada kemungkinan terjadi duplikasi tugas untuk dibagi dalam beberapa segmen jaringan untuk mengurangi *bottleneck.*

(2)Pendefinisian Operasional Jaringan. Langkah yang bagus jika anda mendapatkan perhitungan sumber daya dan pemakaian jaringan. Perhitungan ini berkaitan dengan spesifikasi perangkat keras yang akan dipakai seperti apakah harus menggunakan *switch* daripada *hub*, seberapa besar memory yang dibutuhkan, apakah dibutuhkan kabel *riser fiber optik* karena jaringan menyangkut bangunan berlantai banyak, dan sebagainya.

(3)Pendefinisian Administrasi Keamanan. Tipe keamanan jaringan berkaitan banyak dengan jenis autentifikasi dan data dalam jaringan. Selain ancaman terhadap jaringan dari arah luar juga harus diperhatikan ancaman dari arah dalam, dari pengguna jaringan itu sendiri. Pertimbangan terhadap keamanan ini juga mempengaruhi pemakain peralatan baik secara fisik dan logik. Secara fisik misalnya penggunaan *switch* lebih aman terhadap proses *sniffing* dari satu *node* ke *broadcast* jaringan, selain meningkatkan kinerja jaringan (pengurangan *broadcast* yang berlebihan), secara logika misalnya penggunaan protokol jaringan yang dipakai (apakah cukup protokol TCP/IP saja?), pemakaian protokol yang *secure* yang dienkrip seperti SSH (*Secure Shell*), SSL (*Secure Socket Layer*) dan PGP (*Pretty Good Privacy*).

(4)Pendefinisian Administratif Jaringan. Untuk kelancaran operasional jaringan harus ada pembagian tugas dalam *maintenance* jaringan, baik yang menyangkut perangkat lunak, standar prosedur maupun yang berkaitan dengan sumber daya manusia seperti *administrator*

dan operator. Aspek-aspek yang berkaitan dengan operasional ini antara lain:

a) Perawatan dan *backup*, kapan, siapa dan menggunakan apa.
b) Pemantauan *software* dan *upgrade* untuk memastikan semua *software* aman terhadap *bugs*.
c) Standar prosedur untuk kondisi darurat seperti mati listrik, *virus* ataupun rusaknya sebagian dari alat.
d) Regulasi yang berkaitan dengan keamanan, seperti *user* harus menggunakan *password* yang tidak mudah ditebak atau penggantian *password* secara berkala.

2.2. Infrastruktur

Menurut Grigg Neil dalam bukunya yang berjudul "*Infrastructure Engineering and Management*" Prasarana yang disediakan oleh perusahaan atau tempat umum sebagai fasilitas yang dapat digunakan dan diberikan secara gratis. Infrastruktur merujuk pada sistem fisik yang menyediakan transportasi, pengairan, drainase, bangunan-bangunan gedung dan fasilitas publik yang lain yang dibutuhkan untuk memenuhi kebutuhan dasar manusia dalam lingkup sosial dan ekonomi.

Masih menurut Grigg Neil dan temannya Fontane G. Darrel dalam seminarnya yang berjudul "*Paradigm & Strategy of Infrastructure Management*", sistem infrastruktur merupakan pendukung utama fungsi-fungsi sistem sosial dan ekonomi dalam kehidupan sehari-hari masyarakat. Sistem infrastruktur dapat didefinisikan sebagai fasilitas-fasilitas atau struktur-struktur dasar, peralatan-peralatan, instalasi-instalasi yang dibangun dan yang dibutuhkan untuk berfungsinya sistem sosial dan sistem ekonomi masyarakat.

Robert J. Kodoatie, 2003 berpendapat definisi teknik juga memberikan spesifikasi apa yang dilakukan sistem infrastruktur dan

mengatakan bahwa infrastruktur adalah aset fisik yang dirancang dalam sistem sehingga memberikan pelayanan publik yang penting.

2.3. *Network*

Network atau jaringan komputer adalah beberapa komputer yang saling terhubung satu sama lain untuk bisa saling berkomunikasi. Tujuan dari *network* adalah agar komputer bisa saling berbicara dan membagi *file* antara satu dengan yang lainnya.

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program – program, penggunaan bersama perangkat keras seperti printer, *harddisk*, dan sebagainya. Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan. Manfaat yang didapat dalam membangun jaringan komputer, yaitu :

- *Sharing resources*

  Sharing resources bertujuan agar seluruh program, peralatan atau *peripheral* lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pengaruh dari pemakai.

- Media Komunikasi

  Jaringan komputer memungkinkan terjadinya komunikasi antar pengguna, baik untuk *teleconference* maupun untuk mengirim pesan atau informasi yang penting lainnya.

- Integrasi Data

  Jaringan komputer dapat mencegah ketergantungan pada komputer pusat, karena setiap proses data tidak harus dilakukan

pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya. Oleh sebab inilah maka dapat terbentuk data yang terintegrasi yang memudahkan pemakai untuk memperoleh dan mengolah informasi setiap saat.

- Pengembangan dan Pemeliharaan

  Pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya, karena setiap pembelian komponen seperti printer, maka tidak perlu membeli printer sejumlah komputer yang ada tetapi cukup satu buah karena printer itu dapat digunakan secara bersama – sama. Jaringan komputer juga memudahkan pemakai dalam merawat *harddisk* dan peralatan lainnya, misalnya untuk memberikan perlindungan terhadap serangan *virus* maka pemakai cukup memusatkan perhatian pada *harddisk* yang ada pada komputer pusat.

- Keamanan Data

  Sistem jaringan komputer dapat memberikan perlindungan terhadap data. Karena pemberian dan pengaturan hak akses kepada para pemakai, serta teknik perlindungan terhadap *harddisk* sehingga data mendapatkan perlindungan yang efektif.

- Sumber Daya Lebih Efisien dan Informasi Terkini

  Dengan pemakaian sumber daya secara bersama – sama, akan mendapatkan hasil yang maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera langsung diketahui oleh setiap pemakai (John Gage, 1984).

2.4. Jenis *Network*

Dijelaskan dalam buku "*Jaringan Komputer*" oleh Andi Kristanto, tentang jaringan komputer secara geografis dibedakan menjadi tiga kelompok:

2.4.1. *LAN* (*Local Area Network*)

Local Area Netowork (LAN), merupakan jaringan yang bersifat internal dan biasanya milik pribadi dalam sebuah perusahaan kecil atau menengah dan biasanya berukuran sampai beberapa kilometer. *LAN* seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalamn kantor suatu perusahaan atau pabrik-pabrik untuk pemakain sumber daya bersama (*resource*,baik *hardware* maupun *software*) serta saran untuk bertukar informas.

2.4.2. *Metropolitan Area Network* (*MAN*)

MAN adalah sebuah jaringan menggunakan teknologi yang sama dengan *LAN*, hanya ukurannya biasanya lebih luas dari pada *LAN* dan biasanya. *MAN* dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau antar kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. *MAN* mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan dengan jaringan televisi kabel

2.4.3. *Wide Area Network* (*WAN*)

Wide Area Network (*WAN*), jangkauannya mencakup daerah geografis yang lebih luas, seringkali mencakup sebuah negara bahkan benua. *WAN* terdiri dari kumpulan *LAN*, *MAN* dan mesin-mesin yang bertujuan untuk menjalankan program aplikasi pemakai.

2.5. Security (Network Security)

Security dengan kata lain bisa disebut dengan penjaga, penjaga seperti apakah yang dimaksud, *security* yang dimaksud disini adalah *security network*, dimana suatu sistem jaringan harus terjaga keamanannya, agar terhindar dari serangan-serangan yang merugikan seperti, *IP address spoofing*, *source routing attacks*, atau *tiny fragment attacks*. *Security* jaringan tidaklah berbentuk secara wujud seperti manusia, namun berbentuk suatu perangkat keras yang dapat mengatur-mengatur segala yang lewat didalamnya, atau biasa dikenal dengan *firewall*. Apa itu *network security*? Bagaimana hal tersebut bisa melindungi jaringan anda? Bagaimana hal tersebut bekerja? dan apa keuntungan menggunakan *network security* dalam bisnis?. *network security* adalah beberapa aktifitas yang dirancang untuk melindungi jaringan, khususnya melindungi kegunaan, kehandalan, integritas, dan keamanan jaringan data anda. *Network Security* efektif dalam melindungin bermacam ancaman dan menghentikan penyebaran ancaman tersebut.

2.6. *Firewall*

Firewall merupakan suatu cara atau mekanisme yang di terapkan, baik terhadap *hardware*, *software*, maupun sistem itu sendiri dengan tujuan untuk melindungi, baik untuk menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan *workstation*, server, *router*, atau *Local Area Network* (*LAN*). Seluruh hubungan/kegiatan dari dalam keluar atau sebaliknya harus melewati *firewall*. Hal ini dapat dilakukan dengan cara memblok atau membatasi secara *virtual*. Hanya kegiatan yang terdaftar atau dikenal yang dapat melewati atau

melakukan hubungan, hal ini dapat dilakukan dengan cara mengatur *policy* pada konfigurasi keamanan.

Menurut Hendra Wijaya dalam bukunya yang berjudul "Belajar Sendiri Cisco Adsl Router, Pix Firewall, Dan Vpn", dia menjelaskan dan memberi contoh, dalam sebuah konstruksi bangunan, *firewall* dirancang untuk menjaga penyebaran api atau kebakaran dari salah satu bagian gedung kebagian lainnya. Secara teori, sebuah *internet* melayani tujuan-tujuan yang sama, membendung ancaman-ancaman bahaya *internet* menyerang jaringan internal anda.

2.7. Access List

Access list adalah pengelompokan paket berdasarkan kategori. *Access list* bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas *network. Access list* menjadi *tool* pilihan untuk pengambilan keputusan. Penggunaan *access list* yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan. *Access list* digunakan untuk bertujuan untuk memfilter *IP address*, mendefinisikan trafik ke dalam *NAT* atau enkripsi, atau mem*filter non-protocol* seperti *Apple Talk, IPX*, dan lain-lain. Konsep dasar *access list*, *access list* tidak lain adalah daftar kondisi yang dirancang sedemikian rupa oleh *administrator* untuk mengontrol akses-akses ke dan dari *interface router*. Setidaknya terdapat tiga *rule* yang berlaku bagi paket-paket saat berhubungan dengan *access list* :

1. Setiap paket akan dibandingkan dengan setiap baris rancangan *access list* secara berurut.
2. Begitu menemukan kondisi yang sesuai, paket akan beraksi mengikuti dan selanjutnya memperlihatkan batasan-batasan yang diberikan

3. Akan berlaku kondisi "*deny*" pada setiap akhir *access list*, jadi jika sebuah paket tidak menemukan kesesuaian dalam setiap baris rancangan *access list*, paket akan dibuang.

Terdapat dua tipe *access list* yaitu *Standard Access List* dan *Extended Access List*,

- *Standard Access List*: hanya digunakan untuk *filtering IP/IPX address* sumber (*source*)
- *Extended Access List*: dapat mengizinkan atau memblok paket-paket berdasarkan protokol-protokolnya, *IP/IPX address number* dan tujuan, *port-port TCP/UDP* sumber dan tujuan, tipe-tipe pesan *ICMP* atau *IGMP*. *Extended access list* juga men-*support logging* secara selektif.

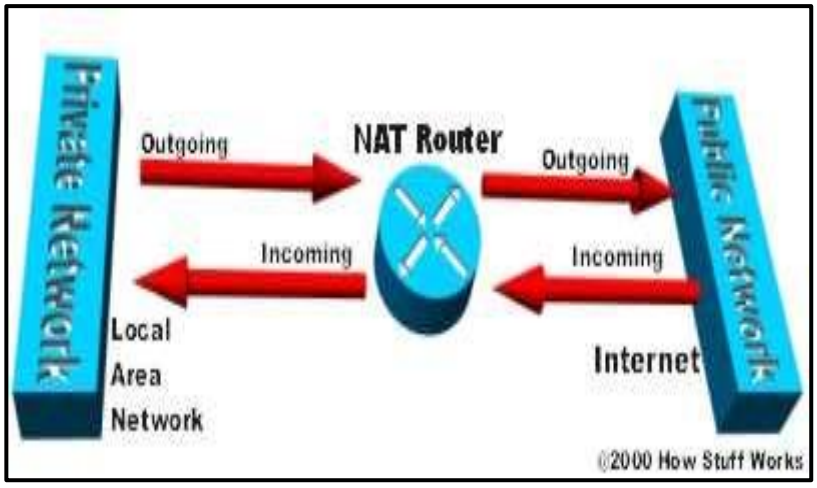
Satu hal lainnya yang perlu dimengerti dalam *access list* yakni inbound *access list* dan *outbond access list*.

- *Inbound Access list* : dalam *inbound access list*, paket-paket diproses melalui *access list* sebelum mereka diarahkan ke *interface outbound*
- *Outbond Access list* : merupakan kebalikan dari *inbound*, yakni paket-paket diarahkan *interface* outbound dan kemudian diproses melalui *access list*.

Kedua parameter diatas adalah parameter yang pasti dipakai dalam melakukan konfigurasi *access list*. Jika parameter *"in"* dan *"out"* tidak diketik, maka *"out"* adalah parameter *default* yang dipakai. Parameter *"in"* dan *"out"* ditunjukan untuk akses masuk atau keluar *interface* dan bukan untuk akses ke jaringan (Wijaya Hendra, 2006).

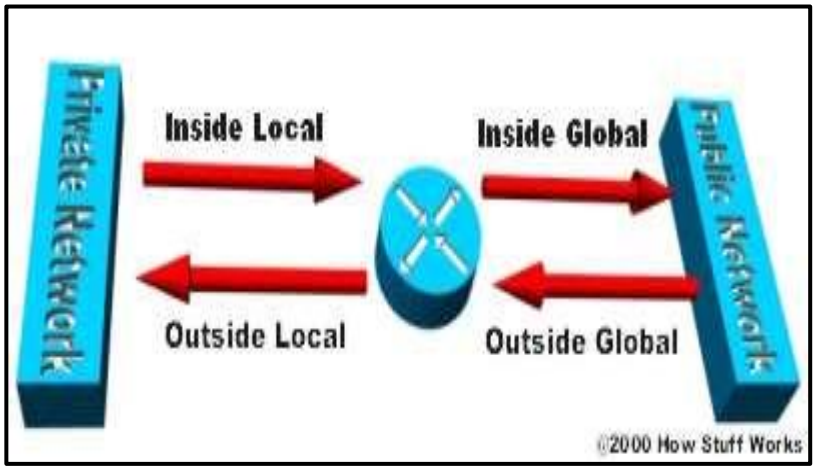
2.8. *NAT*(*Network Address Translation*)

Dalam rangka penghematan *IP public*, dimana jumlahnya yang semakin sedikit, maka diperlukan lah suatu cara untuk menghemat keberadaan *IP public* meskipun telah ada *IPv6* yang siap menggantikan *IPv4* jika jumlahnya memang telah benar-benar habis, namun untuk menggunakan *IPv6* memerlukan beberapa modifikasi infrastruktur. *NAT* menerjemahkan *IP private* yang ada dalam suatu jaringan *network* menuju *IP public*, agar suatu jaringan lokal dapat dipublikasikan sesuai keperluan. *Inside* dan *outside* dalam *NAT* berperan dalam pengembalian paket, siapa yang me-*request* maka akan dikembalikan ke asalnya, tapi pengaturan *inside* dan *outside*, ibarat seseorang yang pergi, tidak mengetahui jalan kembali.



Gambar 2.1 *flow NAT*

dari gambar terlihat bagaimana alur suatu *NAT* mengirimkan suatu *request* ke *public network*, dan mengembalikan paket tersebut ke dalam *private network*.



Gambar 2.2 *Inside* dan *Outside NAT*

setiap *IP private* maupun *IP public* memliki *inside* dan *outside*, karena dibalik *IP public* yang di-*request* juga memilik *IP private* dibaliknya. Ada dua tipe *NAT* yang dapat dipakai, yaitu :

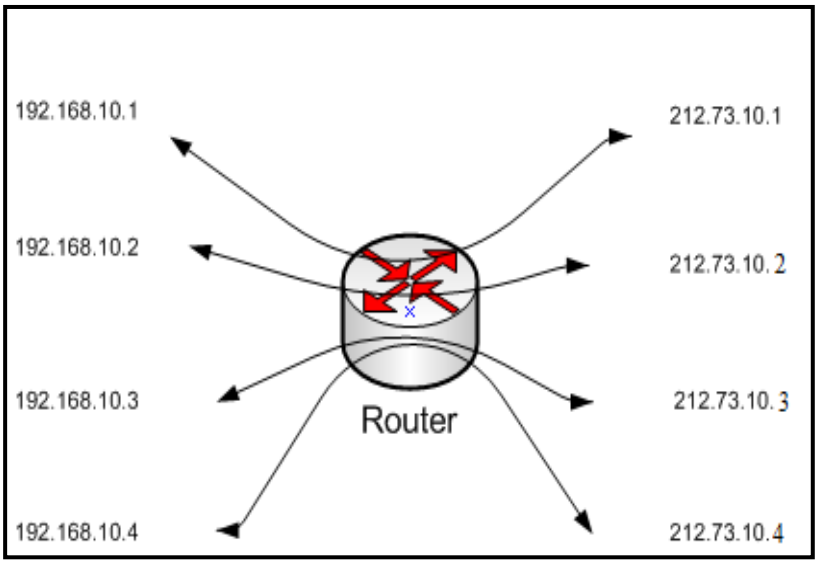
- *Static NAT* : setiap *IP address* pribadi ditranslasikan secara tetap dengan satu *IP* publik tertentu.
- *Dynamic NAT* : setiap *IP address* pribadi ditranslasikan secara dinamis dengan satu *IP address* publik yang tersedia.

2.8.1. Static NAT

Pada *static NAT*, setiap *IP address* pribadi ditranslasikan secara tetap dengan satu *IP address* publik tertentu. Sebagai contoh perhatikan gambar 5.3, komputer-komputer diberikan *IP address* pribadi (192.168.10.1 sampai 192.168.10.4).

Peralatan *router* memiliki dua sisi. Sisi luar (*outside*) memiliki *IP address* publik yang berhubungan dengan *internet* dan sisi dalam memliki *IP address* pribadi yang berhubungan dengan *LAN*. Prinsip kerja *NAT* sangan sederhana, secara manual anda membuat agar *NAT* mentrasnlasikan setiap *IP address* pribadi yang dimilik oleh komputer dengan suatu *IP*

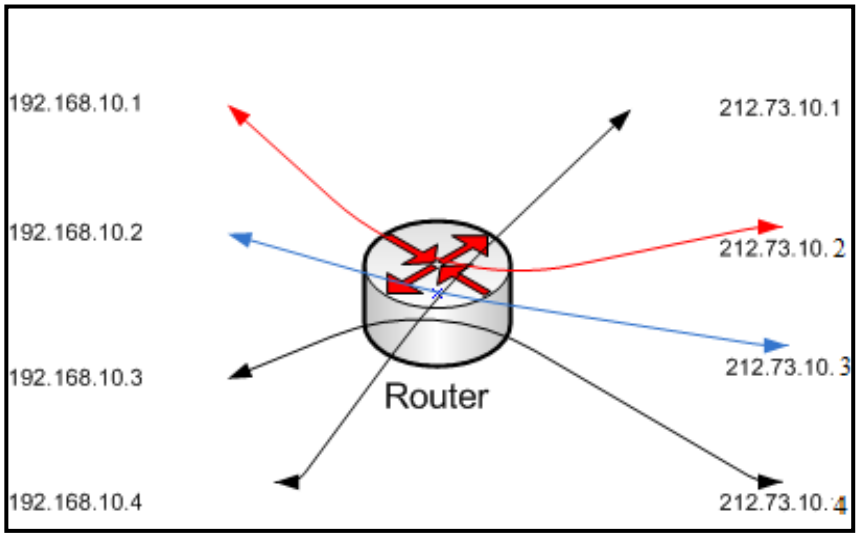
address publik yang anda miliki seperti terlihat pada gambar 2.1.



Gambar 2.3 Translation Static *NAT*

2.8.2. Dynamic NAT

Adakalanya anda menginginkan agar satu kelompok *IP address* pribadi ditranslasikan ke satu kelompok *IP address* publik secara otomatis oleh *NAT*. apabila salah satu *IP address* pribadi dari kelompok akan di pakai, maka *IP address* pribadi tersebut akan ditranslasikan pada *IP address* publik pertama yang mana saja tersedia seperti tampak pada gambar 2.4.

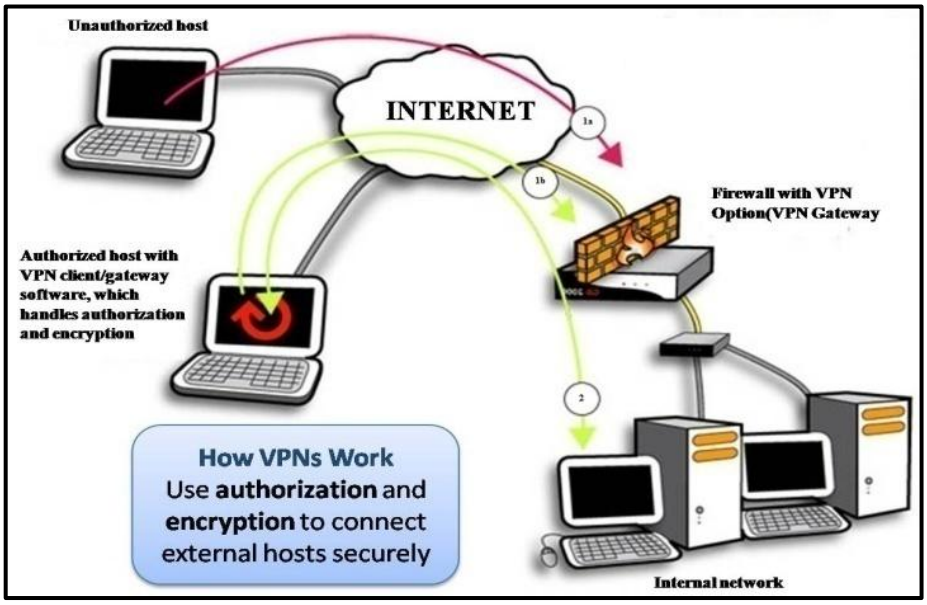


Gambar 2.4 *Translation Dynamic NAT*

Jadi translasi hanya terjadi jika sedang dipakai. Oleh sebab itu translasi berubah-ubah sesuai dengan kebutuhan. *NAT* tipe ini disebut *dynamic* karena berubah-ubah. Keuntungan tipe *dynamic NAT* ini adalah jumlah *IP address* publik yang diperlukan oleh lebih sedikit dari jumlah *IP address* pribadi yang anda miliki, karena pada umumnya tidak semua *IP address* pribadi akan dipakai pada saat yang bersamaan.

2.9. VPN (Virtual Private Network)

VPN adalah jaringan *private* yang dibangun dalam infrastruktur jaringan publik, seperti jaringan *internet*. Sifat lain *VPN* yaitu mengizinkan terjadinya koneksi secara *virtual* dan *private*. *VPN* tidak sepenuhnya terpisah dari jalur utama *network*, hal itu disebabkan karena *VPN* beroperasi dalam satu infrastruktur utama yang sama. *VPN* menyediakan lingkungan komunikasi secara eksklusif namun tidak berbagi terhadap koneksi lain. *VPN* adalah suatu lingkungan komunikasi yang memiliki hak akses untuk mengendalikan *peer-connections* bagi mereka yang berkepentingan, dan dibangun melalui sebagian jaringan.



Gambar 2.5 *flow VPN*

Secara singkat, *VPN* adalah pembangunan jalur koneksi secara *private* dan *virtual* untuk akses ke dalam suatu jaringan yang diizinkan untuk diakses oleh orang-orang yang berkepentingan, dengan menggunakan koneksi utama.

2.10. ***Cisco ASA 5500 Series* (5510)**

Cisco® ASA 5500 *Series Adaptive Security Appliances* memberikan sederetan integrasi keamanan yang sangat kuat, cocok untuk bisnis berskala kecil dan menengah, perusahaan-perusahaan, *service provider*, serta tempat-tempat yang bersifat kritikal, seperti data *center*.

Cisco Asa 5510 *Adaptive Security Appliance* memberikan performa kinerja *firewall* yang tinggi serta dapat membuat *service VPN*, memiliki 5 *port fast ethernet* 10/100. Kapasitas *VPN* yang dapat ditingkatkan dengan menambahkan kemampuan *clustering VPN* dan *load-balancing*, dengan membeli *license*. Berikut *Table lists features of the Cisco* Asa 5510.

Feature	*Description*
Firewall Throughput	*Up to 300 Mbps*
Maximum Firewall and IPS Throughput	*• Up to 150 Mbps with AIP SSM-10* *• Up to 300 Mbps with AIP SSM-20*
VPN Throughput	*Up to 170 Mbps*
Concurrent Sessions	*50,000; 130,000*[1]
IPsec VPN Peers	*250*
Premium AnyConnect VPN Peer License Levels[2]	*2,10, 25, 50, 100, or 250*
Security Contexts	*Up to 5*[3]
Interfaces[*]	*5 Fast Ethernet ports; 2 Gigabit Ethernet + 3 Fast Ethernet*[*]
Virtual Interfaces (VLANs)	*50; 100*[*]
Scalability[*]	*VPN clustering and load balancing*
High Availability	*Not supported; Active/Active*[4]*, Active/Standby**

Tabel 2.1 List Features of Cisco Asa 5510

[1]*Upgrade available with Cisco Asa 5510 Security Plus license*

[2]*Separately licensed feature; includes two with the base system*

[3]*Separately licensed feature; includes two with the Cisco Asa 5510Security Plus license*

[4]*Available for the firewall feature set*

2.11. Topologi

Topologi jaringan menjelaskan struktur dari suatu jaringan komputer. Satu bagian dari definisi topologi adalah *physical* topologi, dimana merupakan suatu *layout* aktual dari kabel, atau media. Bagian lainnya adalah *logical* topologi, yang menjelaskan bagaimana *host-host* mengakses media untuk mengirim data.

Secara sederhana, topologi menggambarkan struktur dari suatu jaringan, atau bagaimana suatu jaringan didesain. Topologi secara fisik adalah rancangan topologi tersebut dapat dilihat dengan mata dan keberadaannya dapat dipastikan. Sedangkan topologi *logical* adalah, topologi yang wujudnya tidak ada secara fisik, tidak dapat disentuh, namun ada secara *virtual* dan dapat dituangkan kedalam bentuk gambar.

Memilih jenis kabel yang digunakan untuk membangun jaringan tidak lepas dari jenis topologi yang kita gunakan. Namun intinya, jaringan komputer adalah jaringan kabel dimana bentuk dan fungsi dari jaringan tersebut menentukan pemilihan jenis kabel.

Topologi fisik jaringan adalah cara yang digunakan untuk menghubungkan *workstation-workstation* didalam *local area network*. Ada beberapa topologi jaringan yang didengar pada umumnya, yaitu:

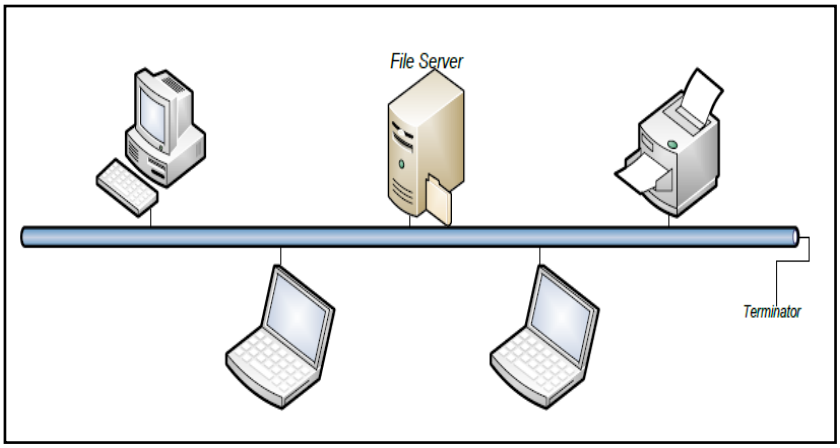
2.11.1. Topologi *Linear Bus* (Garis Lurus)

Topologi *linear bus* terdiri dari satu jalur kabel utama dimana pada masing-masing ujungnya diberikan sebuah *terminator*. Semua *nodes* pada jaringan terkoneksi pada sebuah kabel utama (*backbone*). Jaringan-jaringan *Ethernet* dan *Local Talk* menggunakan topologi ini. Kelebihan dari topologi *linear bus* adalah :

a. Mudah dalam mengkonfigurasi komputer atau perangkat lain ke dalam sebuah kabel utama.
b. Tidak terlalu banyak menggunakan kabel dibandingkan dengan topologi *star* / bintang.

Kekurangan dari topologi *linear bus* adalah :

a. Seluruh jaringan akan mati jika ada kerusakan pada kabel utama.
b. Membutuhkan *terminator* pada kedua sisi kabel utamanya.
c. Sangat sulit mengidentifikasi permasalahan jika jaringan sedang *down* atau rusak.
d. Sangat tidak disarankan dipakai sebagai salah satu solusi pada penggunaan jaringan di gedung besar.



Gambar 2.6 Topologi Linear Bus

Pada gambar 2.6 memperlihatkan topologi jaringan *linear bus*, pada gambar tersebut kita dapat melihat *backbone* dan *termiNATor* dari *backbone*.

2.11.2. *Star* (Bintang)

Topologi model ini dirancang yang mana setiap *nodes* terkoneksi ke jaringan melewati sebuah *concentrator*.

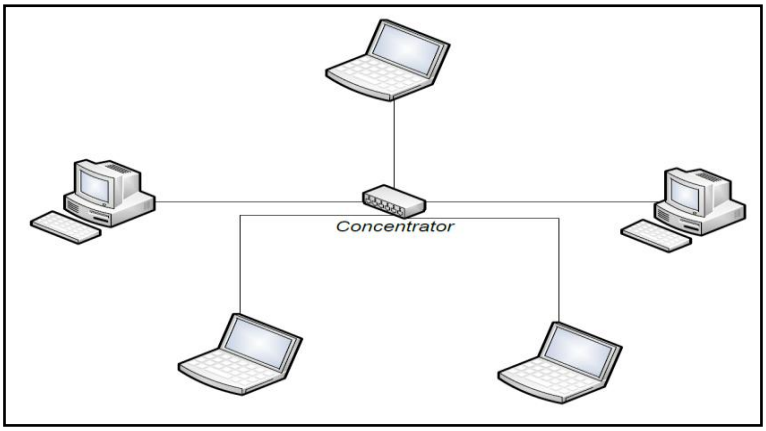
Data yang dikirim ke jaringan lokal akan melewati *concentrator* sebelum melanjutkan ke tempat tujuannya, *concentrator* akan mengatur dan mengendalikan keseluruhan fungsi jaringan dan juga bertindak sebagai *repeater*. Konfigurasi jaringan model ini menggunakan kabel *Twisted Pair* dan dapat digunakan pada kabel *coaxial* atau kabel *fibre optic*.

Kelebihan topologi *Star* (bintang) adalah :

a. Mudah dalam pemasangan dan pengkabelan.
b. Tidak mengakibatkan gangguan pada jaringan ketika akan memasang atau memindahkan perangkat jaringan lainnya.
c. Mudah untuk mendeteksi kesalahan dan memindahkan perangkat-perangkat lainnya.

Kekurangan dari topologi *Star* (bintang) adalah

a. Membutuhkan lebih banyak kabel daripada topologi *linear bus*.
b. Membutuhkan *concentrator* dan apabila *concentrator* rusak maka semua *node* yang terkoneksi tidak dapat terdeteksi.
c. Lebih mahal daripada topologi *linear bus* karena biaya untuk pembelian *concentrator*.

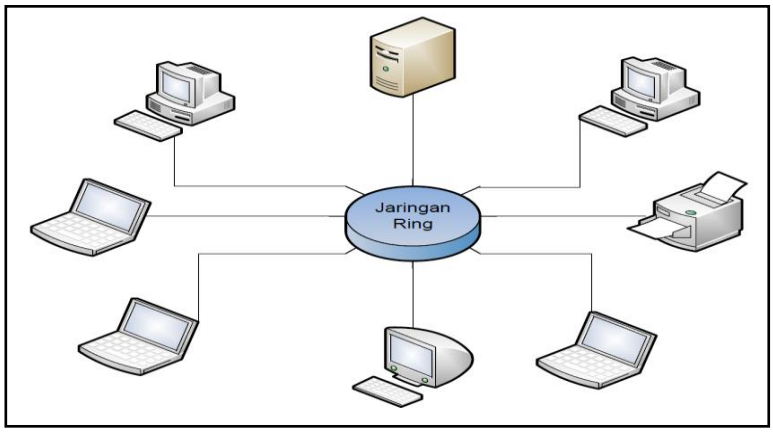


Gambar 2.7 Topologi Star

Pada gambar 2.7 memperlihatkan topologi jaringan *star*, pada gambar tersebut kita dapat melihat *concentrator* yang merupakan bagian paling vital dari topologi ini.

2.11.3. *Ring* (Cincin)

Topologi *Ring* (cincin) menggunakan teknik konfigurasi yang sama dengan topologi *star* tetapi pada topologi ini terlihat bahwa jalur media transmisi menyerupai suatu lingkaran tertutup menyerupai cincin sehingga diberi nama topologi bintang dalam lingkaran atau *star-wired ring*.



Gambar 2.8 Topologi *Ring*

Pada gambar 2.8 di atas terlihat bahwa *concentrator* dari topologi *ring* berbentuk lingkaran tetapi sebenarnya yang berbentuk lingkaran itu adalah kabel untuk menghubungkan dari kartu jaringan ke *concentrator*

2.11.4. *Tree* (Pohon)

Topologi model ini merupakan perpaduan antara topologi *linear bus* dan *star*, yang mana terdiri dari kelompok-kelompok *workstation* dengan konfigurasi *star* yang terkoneksi ke kabel utama yang menggunakan topologi *Linear Bus*. Topologi ini memungkinkan untuk

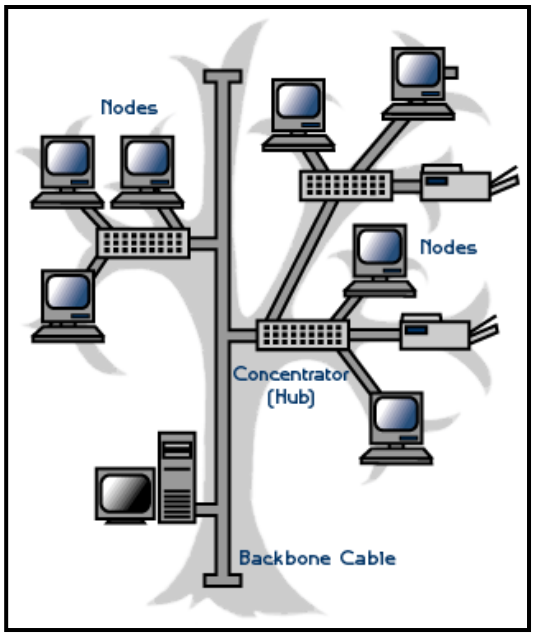
pengembangan jaringan yang telah ada dan memungkinkan untuk mengkonfigurasi jaringan sesuai dengan kebutuhan.

Kelebihan dari topologi *Tree* adalah

a. Proses konfigurasi jaringan dilakukan dari titik ke titik pada masing-masing segmen.
b. Didukung oleh banyak perangkat keras dan perangkat lunak

Kekurangan dari topologi *tree* adalah :

a. Keseluruhan panjang kabel pada tiap-tiap segmen dibatasi oleh tipe kabel yang digunakan.
b. Jika jaringan utama rusak maka keseluruhan segmen ikut rusak juga.
c. Sangat relatif sulit untuk dikonfigurasi dan proses pengkabelannya dibandingkan dengan topologi jaringan yang lain.



Gambar 2.9 Topologi Tree

Pada gambar 2.9 di atas terlihat bahwa topologi *tree* merupakan gabungan dari beberapa topologi.

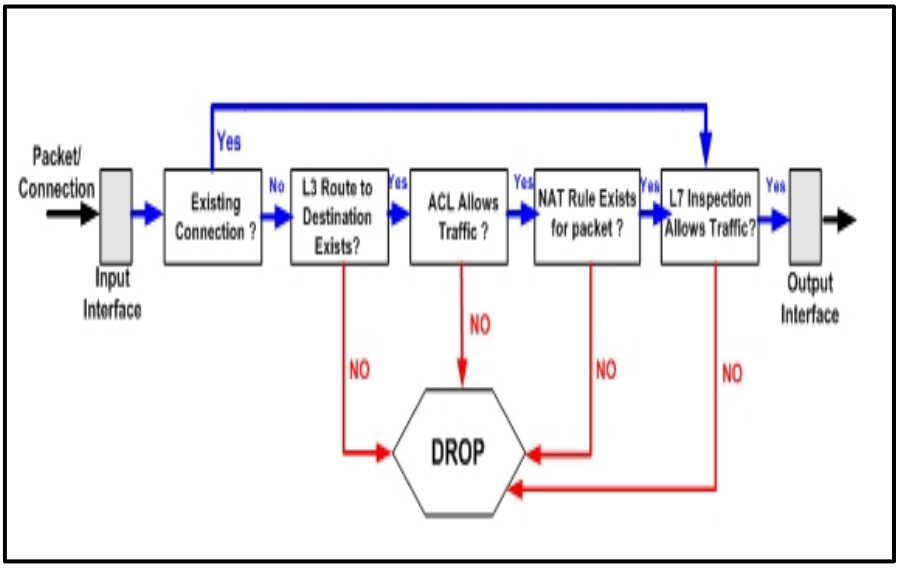
2.12. TCP/IP

TCP/IP adalah sekumpulan protocol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada *Wide Area Network* (*WAN*). *TCP/IP* adalah program 2 *layer*, *layer* yang paling atas *Transmission Control Protokol*, (*TCP*) mengatur *assembly* dari pesan atau *file* ke dalam paket-paket yang lebih kecil yang akan ditransmisikan melalui *internet* dan ditererima oleh *TCP layer* yang akan meng-*assembly* paket kedalam pesan atau bentuk yang sebenarnya. *Layer* yang paling bawah *Internet Protocol* (*IP*), menangani bagian alamat dari tiap-tiap paket sehingga akan menjamin paket akan sampai ketujuannya.

2.13. Flow Cisco Asa Firewall

Perangkat *layer* 3, *routing device* yang normal, ketika menerima paket yang masuk ke dalam *interface*, hal pertama yang dilakukan adalah memeriksa tujuan IP *address* dari paket tersebut, kemudian melihat pada *routing table*, untuk menentukan kemana paket ini akan dikirim, dan *interface* mana yang tepat untuk mengirim paket tersebut, itu adalah hal dasar dalam proses *routing*.

Sebuah *stateful firewall* (seperti *Cisco* Asa), memiliki banyak pekerjaan yang lebih rumit yang harus dilakukan pada paket yang masuk. Ada beberapa langkah dan beberapa keputusan untuk menentukan kemana paket akan pergi, sebelum diizinkan dan diteruskan oleh *firewall*, kondisi ini disebut "*condition forwarding*", karena paket harus memenuhi beberapa aturan dan kondisi sebelum melewati *firewall*. Gambar dibawah ini akan menunjukan *traffic* sederhana dari paket yang melalui *Cisco* Asa,



Gambar 2.10 flow *Cisco* Asa

dari gambar yang ditunjukan diatas, paket yang datang dari input *interface*, sedang diperiksa dibagian koneksi yang terhubung, jika paket tersebut lolos *rule* yang berlaku, maka paket tersebut menuju ke tahap berikutnya, dan setelah itu hanya di periksa dan diinspeksi oleh *layer* 7 untuk memenuhi kriteria yang berlaku.

Selanjutnya, jika paket yang datang adalah koneksi yang baru, maka *firewall* perlu menyimpan segala informasi mengenai koneksi yang baru tersebut. Informasi yang disimpan seperti, sumber dan tujuan paket, sumber dan tujuan *port*, TCP *sequence number*, dan lain-lain. Karena paket adalah koneksi yang baru, maka paket tersebut akan melalui beberapa langkah dan pemeriksaan sebelum diteruskan ke *interface* keluar.

Pertama *firewall* akan memeriksa pada *routing table*, apakah ada *route layer* 3 pada paket. Setelah itu, apakah terdapat *access list* pada *interface* yang mengizinkan koneksi tertenu untuk lewat. Jika tahap tersebut telah selesai, maka *firewall* akan melakukan pengecekan apakah ada *rule NAT* yang dibuat untuk koneksi tertentu. Kemudian *firewall* melakukan pengecekan, koneksi tertentu seperti apakah yang

diizinkan lewat. Setelah semua hal tersebut, maka tahap pengecekan paket selesai, dan hanya paket yang sesuai kriteria yang bisa keluar ke *interface* tujuan.

2.14. Mengenal Model Referensi *ISO-OSI*

Dalam dunia komunikasi komputer, kita sering mendengar istilah Model Referensi *ISO-OSI*. Model referensi *ISO* (*International Standardization Organization*) merupakan salah satu aturan dan standar untuk komunikasi komputer. Model referensi *ISO* menggunakan metode lapisan sebagai model referensi. Semua subsistem komunikasi dibagi menjadi tujuh lapisan. Pembagian ini untuk menentukan berbagai macam fungsi dan sistem operasi. Model yang digunakan dalam sistem komunikasi data dikenal dengan *OSI* (*Open System Interconnection*) tujuh *layer*. *OSI* sangat berperan dalam mengidentifikasi sistem komputer untuk melaksanakan pengolahan dan penyaluran data. Struktur model *OSI* dibagi atas tujuh lapisan *(layer).* Masing masing lapisan mempunyai fungsi dan aturan tersendiri. Tujuan pembagian lapisan adalah mempermudah pelaksanaan aturan standar secara praktis. Pembagian ini juga untuk memungkinkan fleksibilitas, artinya apabila terjadi perubahan pada salah satu lapisan maka tidak akan berpengaruh pada lapisan yang lain. (*Kurniawan, 2007:5*).

Gambar 2.11 Model *OSI layer*

(Sumber : *Kurniawan, 2007:5*)

2.14.1. Lapisan Fisik *(Physical Layer)*

Menangani antar muka secara fisik dalam jaringan komputer. *Layer* ini berfungsi dalam pengiriman *raw bit* ke *channel* komunikasi. *Layer* ini memastikan bahwa bila satu sisi mengirim data 1 bit, data tersebut harus diterima oleh sisi lainnya, sebagai 1 bit pula (*Kurniawan, 2007:5*).

2.14.2. Lapisan Data Link *(Data Link Layer)*

Menangani topologi jaringan, pesan kesalahan dan *flow control*. Tugas utama *layer* ini adalah sebagai fasilitas transmisi *raw* data dan mentransformasikan data tersebut ke dalam saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan ke *layer* berikutnya, data link *layer* bertugas memecah-mecah data input menjadi sejumlah data *frame,*

kemudian data *link layer* mentrasmisikan *frame* tersebut secara berurutan, dan memproses *acknowledgement frame* yang dikirim kembali oleh penerima (*Kurniawan, 2007:5*).

2.14.3. Lapisan Jaringan *(Network Layer)*

Bertugas menerapkan *routing* dan memilih *routing*, dengan cara mendapatkan informasi perangkat keras dari nomor *IP* (*Internet Protocol*). Transport *layer* bertugas untuk menerima data dari *session layer*, memecah data menjadi bagian-bagian yang lebih kecil bila perlu, meneruskan data ke *Network layer*, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar (*Kurniawan, 2007:6*).

2.14.4. Lapisan Transport *(Transport Layer)*

Menerapkan layanan transport data andal yang transparan terhadap *layer* diatasnya, contohnya *flow control, multiplexing, management, virtual circuit*, serta *error checking & error recovery* (*Kurniawan, 2007:6*).

2.14.5. Lapisan Session *(Session Layer)*

Berfungsi untuk menetapkan *session* bagi para pengguna dengan pengguna lainnya. *Layer* ini akan membuka, mengatur, dan menutup suatu *session* antara aplikasi-aplikasi (*Kurniawan, 2007:6*).

2.14.6. Lapisan Presentasi *(Presentation Layer)*

Berfungsi untuk melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penyelesaian umum bagi masalah

pada jaringan. Contoh dari *layer* ini adalah telnet untuk protokol akses dari jarak jauh, *SNMP (Simple Network Management Protocol)* untuk manajemen jaringan (*Kurniawan, 2007:6*).

2.14.7. Lapisan Aplikasi *(Application Layer)*

Berfungsi untuk memberikan sarana pelayanan langsung pada *user*, yang berupa aplikasi-aplikasi dan mengadakan komunikasi dari program ke program. Contoh bila ingin *browsing* ke *internet* maka dilakukian dengan membuka aplikasi *browser* (*Kurniawan, 2007:6*).

2.15. Sekilas *Cisco VPN Client*

Cisco VPN Client adalah *software* yang memungkinkan para pengguna *Cisco* untuk membuat koneksi yang aman, "*end-to-end encrypted tunnels*" ke semua "*Cisco Easy VPN Server*".

Cisco Easy VPN, adalah *software* yang dapat membantu melakukan perbaikan pada *Cisco Router*s dan peralatan keamanan *Cisco* lainnya yang telah diterapkan, *VPN* yang sangat sederhana yang diterapkan untuk melakukan *remote* ke kantor dan atau ke pekerja yang berada di lokasi. Berbasis *Cisco Unfied Client Framework*, *Cisco Easy VPN*, memusatkan dan memanagement ke semua peralatan *VPN Cisco*, sehingga mengurangi kompleksitas penerapan *VPN*. *Cisco Easy VPN* memungkinkan untuk melakukan *VPN* ke *VPN remotes*-*Cisco router*s, *Cisco ASA & PIX Security Appliances*, *Cisco VPN software* yang berpusat pada *client* dengan pembuatan *single policy* yang tetap dan *key management method* sehingga sangat sederhana dalam melakukan *remote* ke sisi *administrator*.

BAB 3
GAMBARAN UMUM PERUSAHAAN

3.1. Gambaran Umum Perusahaan

Diambil dari laporan tahunan perusahaan, "PT. Bukit Uluwatu Villa Tbk. adalah perusahaan pengembangan hotel dan resor di Indonesia. Menawarkan pengalaman gaya hidup yang unik berpadu dengan keramah-ramahan dan berfokus pada *trend-setting concepts*, elemen rancangan anggun dan eksklusif. Semua digaris bawahi dengan pelayanan prima untuk kebutuhan para tamu kelas atas.

Berdiri sejak tahun 2000, memiliki visi untuk menjadi pemimpin pasar khususnya dalam resor yang ramah lingkungan. Misi kami adalah mewujudkan desain unik di setiap lokasi resor sambil mendukung komunitas lokal dan kebudayaan setempat. Salah satu mimpi kami ialah merealisasikan potensi industri pariwisata Indonesia yang luar biasa dengan lebih membangkitkan budaya lokal. Kami pun berupaya dan bekerja lebih keras supaya para investor dapat memetik *cash flow* dan *capitar appreciation.*

Dikelola oleh Alila Hotels & Resorts Ltd. (AHR), resor kami menyediakan kegembiraan tiada tara dan pengalaman relaksasi tiada banding bagi para pelancong manca negara, dimana suasana elegan, tenang dan berpadu dengan layanan kelas satu.

Sentuhan inovatif kami dalam memadukan sisi komersil, konservasi, dan komunitas telah berkembang dari properti kami semula yaitu Alila Villas Uluwatu dan Alila Ubud. Akan ada penambahan 12 villa di Alila Ubud. Alila Villas Bintan dan Alila Manado diperkirakan beroperasi ditahun 2013.

Perseroan akan terus melebarkan sayap bisnis dengan menambah jumlah hotel dan villa yang sudah ada di resor kami atau

dengan akuisisi properti lain yang sudah sesuai dengan konsep perseroan".

3.2. Visi dan Misi Perusahaan

- Visi Perusahaan

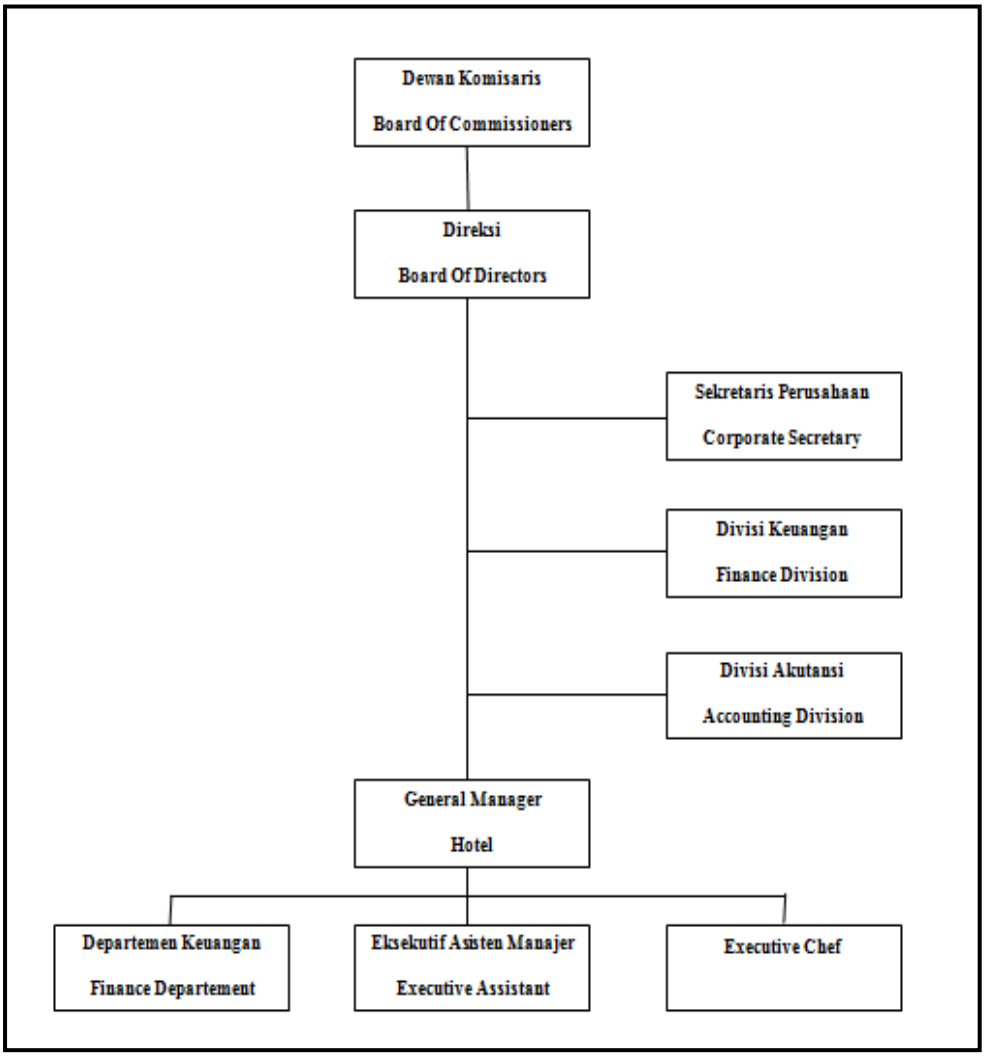
  Menjadi perusahaan terbaik di sektor hotel, *leisure*, dan *lifestyle* yang ramah lingkungan.

- Misi Perusahaan

  1. Membangun resor yang ramah lingkungan, dengan desain yang unik sambil membantu masyarakat setempat dengan mempromosikan seni dan budaya mereka .
  2. Mengembangkan daerah-daerah berpotensial dalam rangka turut serta memajukan pariwisata Indonesia.

3.3. Struktur Organisasi PT. Bukit Uluwatu Villa Tbk

Struktur Organisasi PT. Bukit Uluwatu Villa Tbk. Adalah sebagai berikut :



Gambar 3.1 struktur organisasi alila villas

3.4. Analisis masalah

Pembangunan *firewall* pada hotel bukanlah tanpa tujuan, penulis mencoba memaparkan masalah yang di dapat sebagai berikut :

- Mencegah terjadinya penerobosan ke jaringan internal yang akan dibangun pada hotel tersebut.
- Membangun jaringan yang aman sebagai akses dari jaringan luar menuju ke jaringan internal.

- Memudahkan akses dari jarak yang jauh atau sangat jauh untuk masuk ke jaringan internal.

3.5. Rencana Solusi Pemecahan Masalah

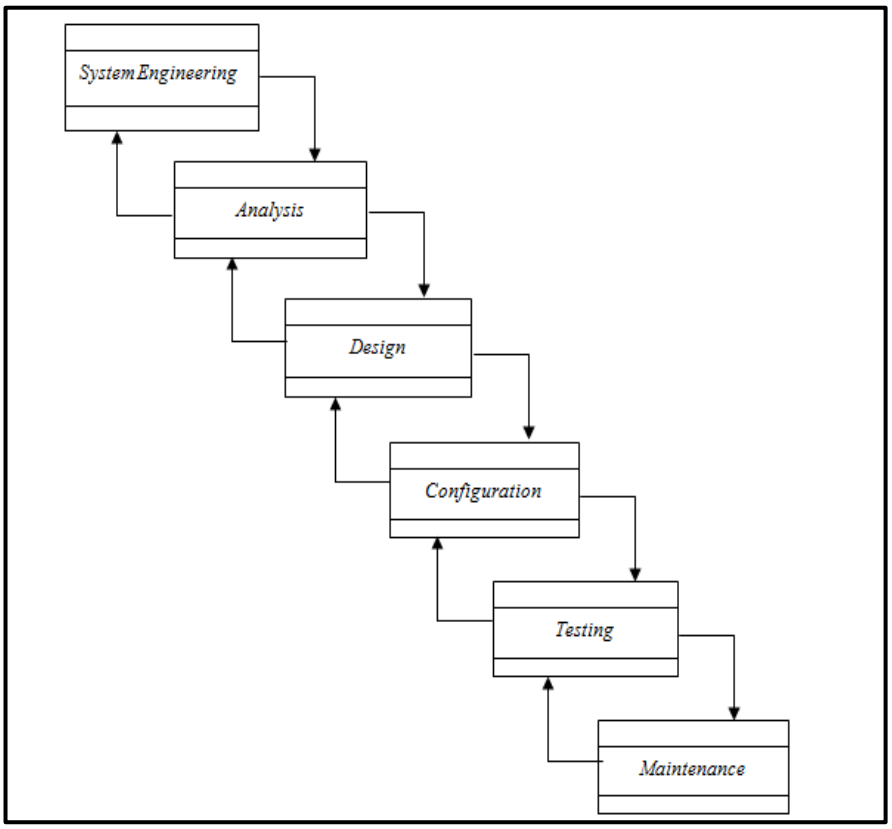
Dari hasil analisis masalah diatas, perlu dilakukan beberapa tahap untuk mengatasi hal tersebut,

- Tahap yang pertama adalah melakukan studi awal dengan menentukan seperti apa penggunaan *firewall* yang ingin diterapkan pada perusahaan. Mempelajari jaringan seperti apa yang ingin diterapkan. Kemudian merancang topologi yang tepat sesuai kebutuhan.
- Tahap yang berikutnya menentukan jalan keluar dari masalah yang ditemukan, untuk me*monitoring traffic*, menggunakan *Netflow Analyzer*.

  Namun *server* untuk memantau tersebut hanya berada pada jaringan lokal, dan tidak bisa diakses dari luar, maka untuk membuat *server* tersebut bisa diakses dari luar, Harus mempergunakan *NAT*.

  Kemudian yang berikutnya adalah, bagaimana *engineer* dapat melakukan konfigurasi dari jarak yang sangat jauh, jika mempergunakan *telnet* tidaklah mungkin, karena telnet memiliki beberapa kelemahan, maka satu-satunya jalan dengan membangun koneksi *VPN* ke dalam jaringan internal, *VPN* jauh lebih baik dibandingkan dengan *telnet*.

3.6. Metodologi Penelitian



Gambar 3.2 Metodologi Penelitian *Waterfall*

Penjelasan :

1) System *Engineer*

   Tahap ini merupakan tahap awal penentuan segala hal apa saja yang harus disiapkan untuk melakukan pengerjaan proyek tersebut.

2) *Analysis*

   Pada tahap ini, menganalisis tentang jaringan yang tersedia atau belum ada, untuk kemudian diterapkan seperti apa jaringan yang akan dibentuk.

3) *Design*

   Design disini adalah, merancang topologi yang tepat dan sesuai sebagai bahan acuan hasil akhir dari pengerjaan proyek.

4) *Configuration*

   Pada tahap ini, merujuk pada tahap sebelumnya, dimana konfigurasi yang dilakukan berdasarkan pada tahap *design*.

5) *Testing*

   Pada tahap ini jelas sekali maksudnya, dimana *testing* dilakukan untuk menguji apakah pengerjaan proyek sudah berhasil mengenai sasaran yang telah ditentukan, jika belum, maka akan kembali ke tahap sebelumnya.

6) *Maintenance*

   Tahap ini dilakukan jika si pengguna meminta untuk dilakukan penambahan suatu konfigurasi pada saat implementasi telah berjalan, maka tahap maintenan ini akan digunakan.

BAB 4

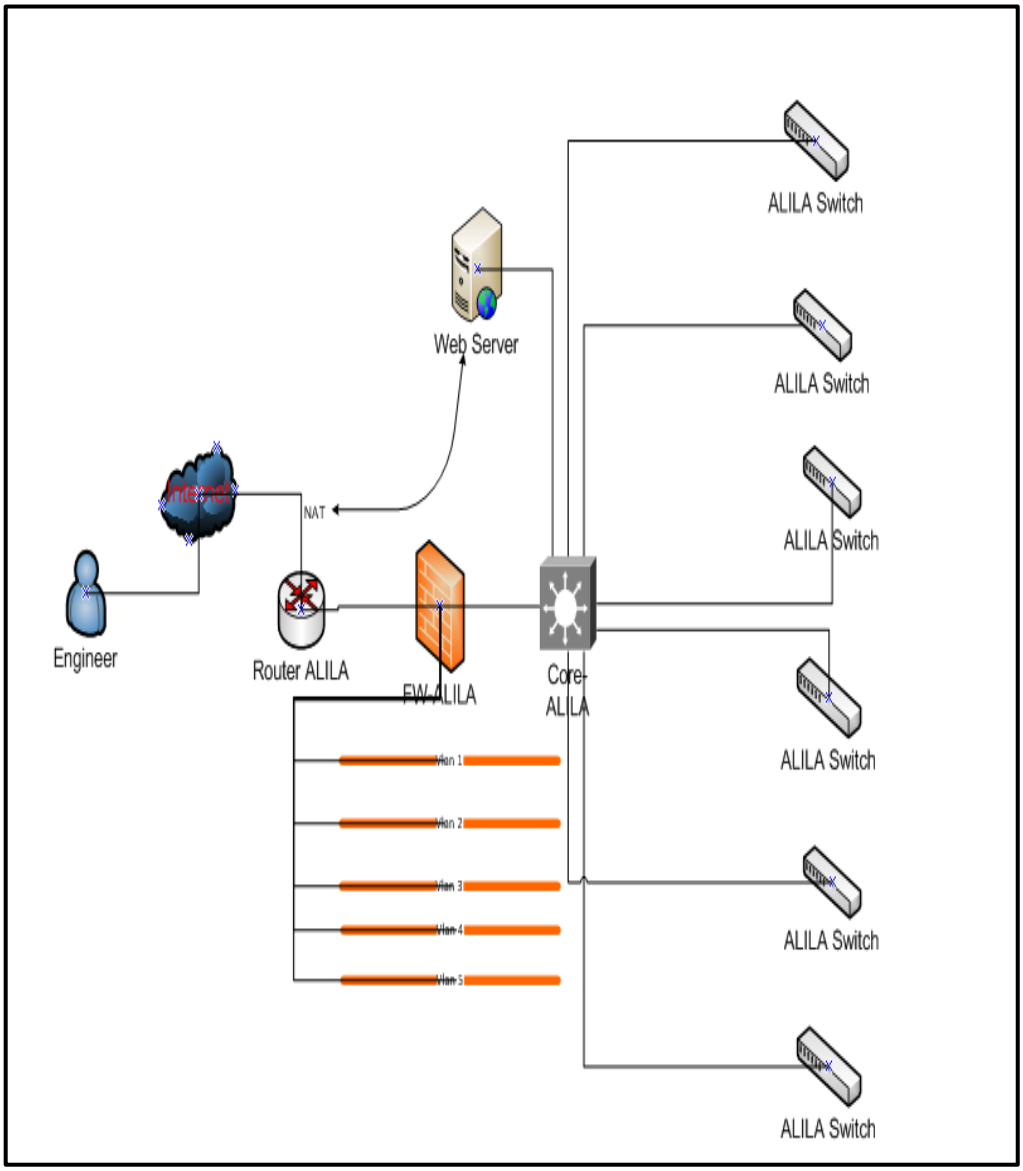
PEMBAHASAN

4.1. Bagaimana merancang topologi jaringan hotel Alila Villas Uluwatu yang handal dari sisi keamanan.

Pada saat kita merancang sebuah jaringan, mungkin kita tidak berfikir untuk melakukan perlindungan secara mendalam terhadap jaringan tersebut, contoh sederhana pada sebuah warnet, mungkin warnet tidak perlu memiliki perlindungan yang mendalam, tapi bagaimana dengan sebuah perusahaan menengah ke atas? Tentu saja mereka memerlukan perlindungan yang lebih mendalam, apalagi jika perusahaan tersebut memiliki induk perusahaan yang memantau keadaan jaringan di salah satu anak perusahaan tersebut.

Dengan menggunakan *router*, bisa saja kita langsung membangun suatu jaringan internal yang terhubung dengan internet, mudah saja, tapi bagaimana jika kita ingin mengakses jaringan internal menggunakan jaringan publik? Bukan tidak mungkin, tetapi sulit, beberapa hal bisa terjadi, seperti penerobosan, perubahan konfigurasi yang seharusnya tidak dilakukan, dan lain sebagainya.

Hotel Alila memiliki topologi seperti gambar 4.1, dimana tidak bisa di pungkiri bahwa *router* tetap berperan dalam topologi tersebut, mengapa demikin, karena penentuan jalur pengiriman data dilakukan oleh si *router*.



Gambar 4.1 Topologi Alila

router berposisi dipaling depan, yang berhubungan langsung dengan internet, mengapa demikian? Karena itulah fungsi utama dari router, me-*routing* paket yang datang dari dalam maupun dari luar.

Pada topologi tersebut *Cisco Asa* berada di posisi setelah *router* dan sebelum jaringan utama dari Alila Uluwatu, mengapa demikian, karena pada pembahasan ini penulis membahas tentang keamanan jaringan, maka dari itu digunakan *firewall*. Mengapa

firewall? Karena sesuai dengan namanya, yaitu dinding, setiap alur lalu lintas jaringan yang menuju ke dan dari dalam akan melalui alat tersebut, untuk melihat paket yang lewat.

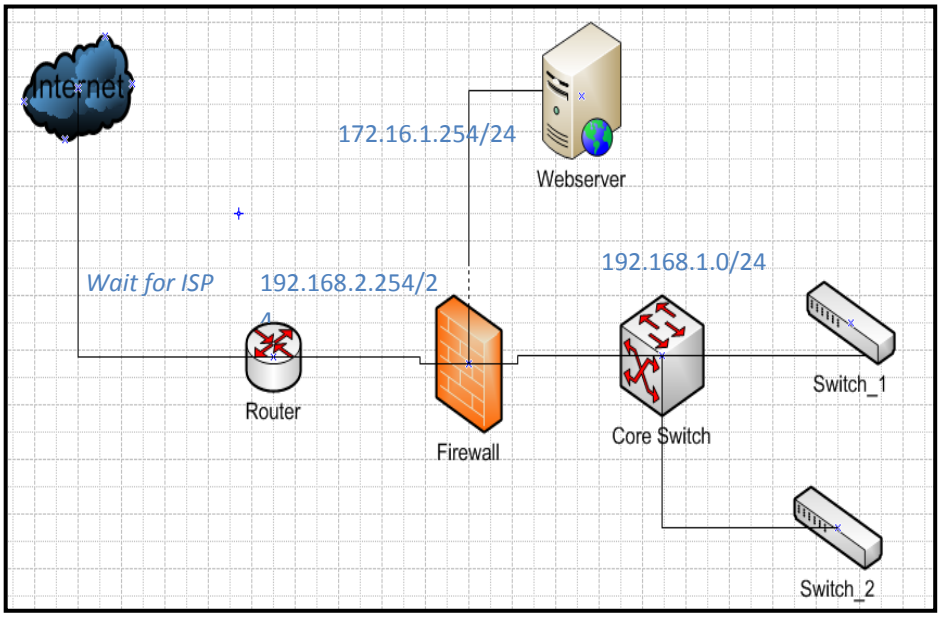
Rancangan tersebut juga berfungsi sebagai *VPN gateway*, dimana akan dibangun jaringan akses pribadi sebagai sarana untuk melakukan perubahan konfigurasi atau semacam itu yang akan dilakukan dari jarak jauh, sehingga tidak perlu berada ditempat itu. Kenapa harus alat itu yang digunakan sebagai pembangunan jaringan akses pribadi? Karena *Cisco Asa* 5510 memiliki kemampuan untuk membatasi siapa saja yang boleh melakukan akses tersebut, untuk itulah alat tersebut dijadikan gerbang akses pribadi.

Alat tersebut juga menterjemahkan alamat pribadi server ke alamat luar, sehingga server tersebut dapat diakses dari luar, dan perusahaan utama pun dapat melihat keadaan jaringa di hotel tersebut. Dan setiap paket yang lewat akan terbaca, baik paket tersebut datang dari luar jaringan maupun dari dalam jaringan, itulah fungsi dari alat tersebut.

Pengerjaan pertama dari pengerjaan topologi ini adalah system *engineering*, dimana menentukan alat yang diperlukan, dalam hal ini, yang pertama dibutuhkan adalah *firewall cisco asa 5510, router cisco1841, switch catalyst 3750,switch catalyst 2960, switch catalyst CE 500.*

Fungsi dari *router cisco1841* adalah sebagai *router* standar yang berfungsi me-*route*, yaitu menentukan arah. Kemudian fungsi dari *switch catalyst 3750* adalah sebagai *core switch* atau *switch* utama yang membagi jadi beberapa bagian. Dan kemudian *switch catalyst 2960* dan *switch catalyst CE 500* berfungsi sebagai switch standar yang membagi jaringan.

Rancangan dari topologi fisik adalah digambarkan seperti yang tertera dibawah ini,



Gambar 4.2 Topologi fisik

Dimana *interface* dari *core switch* diberi *IP Address* 192.168.1.0/24. Dan *web server* diberi *IP Address* 172.16.1.254/24. Dan untuk *interface firewall-router* diberi *IP Address* 192.168.2.254/24. Dan yang terakhir untuk *interface router* menuju *internet,* akan disesuaikan dengan *IP Address* yang didapat dari *ISP*.

Tahap yang kedua adalah *analysis*, apa kebutuhannya, dan seperti apa keinginan dari alila tersebut. Kebutuhan alila adalah ingin menyediakan internet gratis bagi para tamunya, yang ada disetiap kamar, sehingga *user* hanya langsung mencolokan kabel utp, dan langsung terhubung ke internet, dan keinginan dari *corporate* adalah melakukan monitoring traffic dari jarak jauh, dan akses jarak jauh bagi orang-orang yang diperbolehkan.

Tahap yang ketiga atau yang terakhir dalam penulisan ini adalah *design*, dimana rancangan topologi seperti yang dijelaskan diatas, gambaran, fungsi, dan alur dari proses firewall.

Proses dari *firewall* secara default adalah menutup semua port atau memblok semua *policy*, sehingga kemungkinan

penerobosan atau penjebolan dapat diminimalisir, karena mode penyerangan pasti mempunyai tujuan port, dengan *firewall* port yang tidak dideklarasikan secara konfigurasi, akan tertutup.

BAB 5

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari hasil perancangan topologi pada hotel Alila Villas Uluwatu, didapat kesimpulan. Bahwa *Cisco Asa* 5510 akan dijadikan sebagai gerbang utama dalam memonitoring keadaan jaringan, dan dijadikan gerbang utama dalam melakukan akses jaringan pribadi yang aman. Mengapa? Karena *cisco asa 5510* merupakan *firewall security appliance* dan termasuk *statefull firewall,* suatu alat pertahanan jaringan yang tangguh dan kuat yang diterbitkan oleh perusahaan jaringan ternama yaitu *cisco*.

Topologi yang disarankan juga terdapat *switch*, dimana sebagai rencana Alila Uluwatu dalam memberikan internet gratis bagi tamunya.

5.2. Saran

Pada bagian ini penulis akan memberikan beberapa saran kepada Alila Villas Uluwatu, diantaranya :

a. Perlu adanya *maintenance* terhadap alat-alat yang akan digunakan, agar fungsinya tetap berjalan baik.
b. Pembangunan jaringan akses pribadi, hendaknya hanya diberikan kepada orang-orang yang berhak, dikarenakan bersifat rahasia.

DAFTAR PUSTAKA

Andi Kristanto. 2003. *Jaringan Komputer*. Yogyakarta : Graha Ilmu.

Anonim,*http://202.155.2.90/corporate_actions/new_info_jsx/jenis_informasi/01_laporan_keuangan/04_Annual20Report/2010/BUVA/BUVA_Annual%20Report_2010.pdf*, diakses tanggal 3 November 2001

_____,*http://www.Cisco.com/Cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_Network_Security/index.html*, diakses tanggal 9 Oktober 2011

_____,*http://www.Cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html*, diakses tanggal 9 Oktober 2011

_____,*http://www.Cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd8048dba8.html*, 15 November 2011

_____,*http://www.Cisco.com/en/US/products/ps6120/index.html*, diakses tanggal 9 Oktober 2011

_____,*http://www.Cisco.com/en/US/products/sw/secursw/ps2308/index.html*, diakses tanggal 9 Oktober 2011

_____,*http://www.manageengine.com/products/netflow/netflow-monitoring.html*, diakses tanggal 9 Oktober 2011.

Dede Sopandi. 2008. *Instalasi Dan Konfigurasi Jaringan Komputer*. Jakarta : Informatika.

Grigg, Neil, 1988. *Infrastructure Engineering And Management*. John Wiley and Sons.

HM. Jogiyanto.1995.*Analisis & Disain Sistem Informasi*. Yogyakarta : Andi Offset

Nurdin, Syafruddin dan Basyiruddin Usman.2002.*Guru Profesional Dan Implementasi Kurikulum*.Jakarta: Ciputat Pers.

Rika, Michael Yoseph Ricky, _____,*Laboratorium Rumah Sakit Kanker Dharmais Dengan Menggunakan Total Architectur Syntesis, [pdf], http://ict.binus.edu/metamorph/file/research/Paper_Revisi_Renan.pdf, diakses tanggal 14 Oktober 2011*.

Rafiudin, Rahmat.2002.*Menguasai Security Unix*.Jakarta:PT Elex Media Komputindo.

Robert J. Kodoatie, 2003. *Pengantar Manajemen Infrastruktur*.

Wiharsono Kurniawan. 2007. *Jaringan Komputer*. Yogyakarta : Andi.

Wijaya, Hendra (2006). *Belajar Sendiri Cisco Adsl Router, Pix Firewall, Dan Vpn* : 56. Jakarta : Elex Media Komputindo.

KETERANGAN KERJA PRAKTEK

Nama : Nur Ramdhani Siswanto

NIM : 2008-81-116

Nama Perusahaan : Integrasindo Mitra Mandiri

Alamat Perusahaan : Jalan Teluk Betung No 42 Graha Anugerah Lantai 6 Jakarta 10230

Telepon : (021) 40040222

Fax : (021) 3901226

Judul Laporan : Perancangan Topologi Jaringan Menggunakan Cisco Asa 5510 Sebagai Security Pada Hotel Alila Villas Uluwatu.

Tanggal Pelaksanaan : 1 April 2011 – 30 Juni 2011

Mengetahui,

(Yan Martin)	(Fransiskus Adikara,S.Kom.,M.Kom)
Pembimbing Lapangan	Koordinator Kerja Praktek

Integrasindo
PT. Integrasindo Mitra Mandiri
www.integrasindo.co.id

Graha Anugerah 6th Floor Jl. Teluk Betung No. 42
Jakarta Pusat 10230 - Indonesia

Phone : +62 21 390 1224 - 25
Fax : +62 21 390 1226
Email : hello@integrasindo.co.id

LEMBAR PENILAIAN KERJA PRAKTEK

Lembar penilaian ini diberikan kepada,

Nama : Nur Ramdhani Siswanto

NIM : 2008-81-116

Jurusan : Teknik Informatika

Fakultas : Ilmu Komputer

Universitas : Esa Unggul

sebagai hasil akhir dalam melakukan magang dikantor kami, dengan kriteria dan nilai sebagai berikut,

No	Kriteria	Nilai	Paraf
1	Datang On Time	C	
2	Kerapihan	B	
3	Ketekunan	B	
4	Cara Bicara / Menjelaskan	B	
5	Daya Serap / Cepat Tanggap	B	
6	Pengetahuan Tentang Network	B	
7	Responsif	B	

demikian kriteria dan nilai tersebut kami berikan semoga dapat digunakan sebagaimana mestinya.

Mengetahui,

Integrasindo

Pembimbing Lapangan

Yan Martin