BAB II
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Peneliti melakukan studi pustaka terhadap penelitian terdahulu yang relevan dengan penelitian ini agar tidak terjadi kesamaan penciptaan. Penelitian pada tahun 2021 yang berjudul "Perancangan sistem keamanan jaringan untuk Mengurangi kejahatan *cyber* menggunakan teknik *Demilitarized zone* (DMZ) dan *firewall rules* (Studi Kasus: Laboratorium Basis Data IST AKPRIND)" mengangkat masalah bagaimana cara merancang sistem keamaman jaringan untuk mengurangi kejahatan *cyber*. Hasil penelitian ini adalah berhasil memisahkan akses jaringan dosen dan mahasiswa dengan tujuan mengurangi beban *server*[1].

Penelitian pada tahun 2019 yang berjudul "Perancangan Sistem Keamanan Jaringan Pada Universitas Bina Insan Lubuklinggau Menggunakan Teknik *De-Militirazed Zone*". Hasil dari penelitian ini Hasil penelitian ini adalah berhasil melindungi system jaringan internal[2].

Penelitian pada tahun 2017 yang berjudul "Sistem Keamanan Jaringan *Local Area Network* Menggunakan Teknik *De-Militarized Zone*". Hasil dari penelitian ini adalah kebehasilan filter DoS *attack* ICMP, UDP dengan prosentase 98 persen[3].

Penelitian pada tahun 2018 yang berjudul "Optimalisasi Jaringan Menggunakan *Firewall*". Hasil dari penelitian tersebut menunjukkan bahwa *firewall* mampu memberikan perlindungan keamanan jaringan *local* terhadap ancaman dari internet[4].

Penelitian pada tahun 2018 yang berjudul "Uji Kinerja DMZ (*De-Militarized Zone*) dengan Simulator GNS3 (*Grapihical Network Simulator*)*"*. Hasil dari penelitian ini ini adalah dengan *firewall* mampu membatasi akses layanan yang berada di jaringan *local* terhadap akses yang dilakukan dari jaringan internet[5].

Berikut adalah rangkuman penelitian sebelumnya yang sudah ditinjau oleh peneliti dalam bentuk **Tabel 2.1**

Tabel 2.1 Ringkasan Penelitian Terdahulu

No	**Topik Penelitian**	**Pendekatan Metod**	**Hasil**
1	Penelitian pertama, dilakukan oleh Eka Suteja, Erna Kumalasari N, Suwanto Raharjo pada tahun 2021, dengan topik pengamanan jaringan dengan DMZ dan *firewall rules* yang dilakukan di laboratorium basis data Institut Sains Teknologi Akprind.	*Firewall*, DMZ, GNS3, *Iperf*[1]	Hasil penelitian ini adalah berhasil memisahkan akses jaringan dosen dan mahasiswa dengan tujuan mengurangi beban *server*.
2	Penelitian yang kedua, dilakukan oleh M. Agus Syamsul Arifin, Antoni Zulius pada tahun 2019 dengan topik perancangan DMZ pada satu jaringan yang dilakukan di Universitas Bina Insan Lubuklinggau.	*De-Militarized Zone* (DMZ) [2]	Hasil penelitian ini adalah berhasil melindungi *system* jaringan internal.
3	Penelitian ketiga, dilakukan oleh Ino Anugrah, R.Hengki Rahmanto pada tahun 2017 dengan topik pengamanan jaringan *local* dengan Teknik DMZ.	*De-Militarized Zone* (DMZ) [3]	Hasil penelitian ini adalah keberhasilan filter DoS *attack* ICMP, UDP dengan prosentase 98 persen.
4	Penelitian keempat, dilakukan oleh Fajar Adhi Purwaningrum, Agus Purwanto & Eko Agus	*Firewall*[4]	Hasil penelitian tersebut menunjukkan bahwa f*irewall* mampu memberikan

	Darmadi pada tahun 2018 yang mengimplementasikan *firewall* pada jaringan.		perlindungan keamanan jaringan *local* terhadap ancaman dari internet.
5	Penelitian kelima, dilakukan oleh Irma Wira Sari Putri, Lalu Syamsul IrfanA., A. Sjamsjiar Rachman pada tahun 2018 dengan topik uji performa jaringan yang menggunakan DMZ dengan disimulasikan dengan GNS3.	*De-Militarized Zone* (DMZ), *Firewall*[5]	Hasil penilitian ini adalah dengan *firewall* mampu membatasi akses layanan yang berada di jaringan *local* terhadap akses yang dilakukan dari jaringan internet.

2.2 Landasan Teori

2.2.1 Jaringan Komputer

Konsep jaringan komputer merupakan konsep yang dibangun dari dua buah teknologi yaitu komputer dan teknik komunikasi data. Dari dua kemampuan tersebut maka dapat membentuk pengiriman antar komputer melalui jaringan yang saat ini dikenal sebagai jaringan komputer. Dengan kemampuan ini maka jaringan komputer dapat saling berbagi / distribusi layanan / *services* antar komputer. Dengan kemampuan ini maka saat ini komputer tidak berdiri sendiri melainkan mampu berkolaborasi layanan menggunakan jaringan.[7]

Konsep jaringan komputer merupakan komputer yang saling terhubung melalui jaringan komunikasi yang mana mereka mampu berkomunikasi dan berbagi sumber daya, data, dan informasi. [7]

Setiap titik akhir dalam suatu jaringan memiliki tanda pengenal, yang biasa disebut dengan alamat IP atau alamat media *access control*. *Endpoint* dapat mencakup *server*, komputer, telepon, dan perangkat keras (*hardware*) jaringan yang lain. Jaringan komputer (jarkom) dapat dibuat dengan menggunakan gabungan dari teknologi kabel dan *wireless*. Jaringan dapat bersifat privat maupun publik, dalam penggunaan jaringan *private*, biasanya memerlukan akses user untuk memasukkan kredensial berupa kata sandi yang dimasukkan secara manual oleh administrator atau diperoleh langsung oleh pengguna. Untuk penggunaan jaringan publik seperti internet, tidak membatasi suatu akses. [8]

2.2.2 Jenis-jenis jaringan Komputer

Jaringan komputer adalah sebuah jaringan yang dihubungkan secara elektronik antar komputer untuk saling berkomunikasi dengan bertukar data dan berbagi sumber daya satu sama lain. Tujuan dari jaringan komputer adalah agar setiap bagian dari jaringan komputer dapat meminta dan

memberikan layanan. Di bawah ini, jenis-jenis jaringan komputer:

- **PAN (*Pan Area Network*)**

Pengertian jaringan komputer PAN adalah jaringan komunikasi dalam jarak dekat di mana menghubungkan satu perangkat dengan lainnya.Jenis jaringan ini mencakup wilayah yang lebih kecil, misalnya saja pada kantor, dan rumah. Biasanya, banyak digunakan hanya untuk keperluan internet, serta printer. Dan tidak memerlukan *resources* yang besar untuk menggunakan jaringan PAN.

- **LAN (*Local Area Network*)**

Jaringan LAN berfungsi untuk menghubungkan perangkat jaringan dalam kondisi jangkauan yang relatif kecil. Lan merupakan salah satu tipe jaringan komputer yang umum dijumpai. Contoh penerapan jaringan LAN yaitu sistem jaringan pada sekolah, kantor, maupun rumah.Banyak orang yang cenderung menggunakan konektivitas tertentu, terutama pada token ring dan ethernet.Selain itu, LAN juga menyediakan teknologi jaringan wireless dengan menggunakan *Wifi* dan lebih dikenal dengan WLAN (*Wireless Local Area Network*).

- **CAN (*Can Area Network*)**

Pengertian jaringan komputer CAN adalah jaringan yang menghubungkan aneka perangkat dan komputer dalam sebuah instansi pendidikan seperti sekolah, kampus, universitas, dan lain sebagainya. Jaringan CAN dapat dibilang memiliki kesamaan dengan MAN, namun lebih terbatas dalam ruang lingkup kampus atau akademisi. Untuk jaringan ini, lebih banyak digunakan untuk keperluan praktek lab, email, pembaruan kelas, dan lain sebagainya.

- **MAN (*Metropolitan Area Network*)**

MAN adalah jaringan yang menghubungkan antara satu perangkat komputer dengan perangkat yang lain dalam ruang lingkup kota pada jaringan yang

sama. Jenis jaringan ini lebih besar dari dari jaringan LAN.

- **WAN (*Wide Area Network)***

WAN merupakan kumpulan dari LAN yang tersebar secara geografis. Jaringan WAN cenderung untuk menggunakan teknologi seperti ATM, X.25, serta *Frame Relay* untuk konektivitas jarak yang lebih jauh lagi.

- **Internet**

Internet adalah jaringan komputer terbesar yang pernah diciptakan oleh manusia. Ruang lingkup dari internet mencakup hampir seluruh penjuru dunia. Siapapun dapat mengakses berbagai sumber informasi dalam berbagai perangkat komputer, seperti PC, *smartphone*, laptop, tablet, TV, dan lain sebagainya.

- **VPN (*Virtual Private Network)***

VPN merupakan salah satu solusi untuk menyediakan koneksi internet yang lebih aman. VPN dapat membuat jalur aman untuk kebutuhan transmisi data. Saat ini, banyak sekali platform yang menjual VPN secara gratis, maupun menyediakan akses premium.

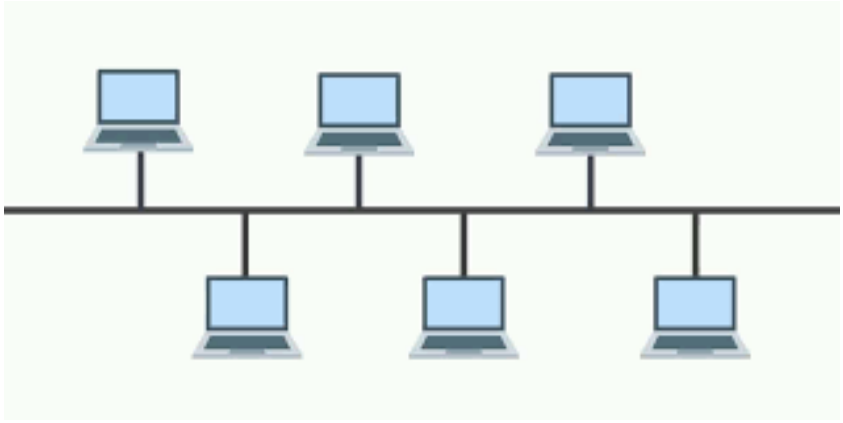
2.2.3 Topologi Jaringan

Topologi jaringan adalah susunan untuk menghubungkan 2 perangkat atau lebih yang terkoneksi antara *node*, dalam sebuah jaringan, secara nyata dan simulasi. Topologi memperlihatkan suatu cara yang digunakan dalam melakukan penyambungan kabel secara fisik di dalam jaringan. Terdapat macam-macam bentuk topologi yang biasanya ada di dalam konsep skalabilitas jaringan antara lain *Local Area Network*, *Bus*, *Ring*, *Star*, dan topologi *Tree (Hybrid)*. Bentuk-bentuk topologi dalam jaringan nyata, antara lain :

2.2.3.1 Topologi Bus atau Linear

Topologi bus banyak digunakan ketika kabel *coaxial* banyak yang menggunakan. Sifat topologi ini yaitu terdapat pengubung yang kedua ujungnya ditutup dan sepanjang penghubungnya terdapat *node-node*, paling lazim karena kesederhanaan diproses instalasi, signal melewati kabel 2 arah yang mungkin terjadi *collision*.

Topologi bus merupakan topologi yang mempunyai kabel tunggal yang masing – masing *workstation* dan *server* saling terhubung. Kelebihan dari topologi bus sendiri yaitu ketika melakukan pengembangan jaringan dan *workstation* baru, akan tetapi tidak mengganggu *workstation* yang lain. Kekurangan yang dimiliki adalah ketika kabel mengalami kerusakan atau putus, maka akan mengalami gangguan pada keseluruhan jaringan.



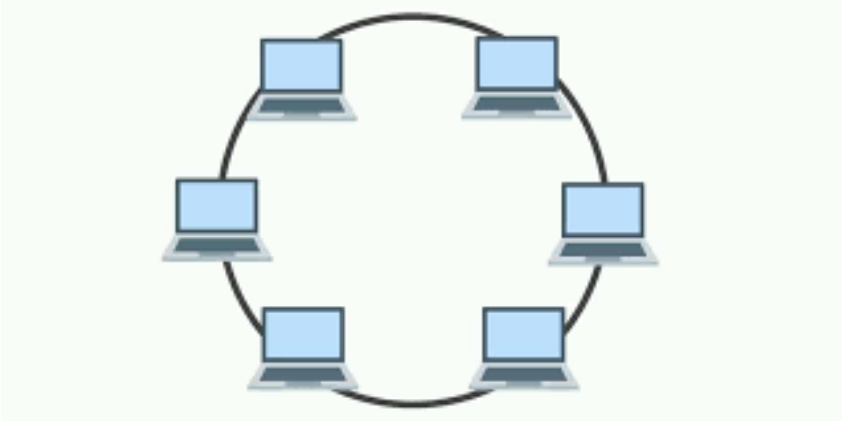
Gambar 2.1 Topologi Bus

2.2.3.2 Topologi Ring

Topologi ring merupakan topologi yang bentukannya seperti cincin atau melingkar. Jenis topologi ini memanfaatkan *fiber optic* sebagai sarananya. Ciri-ciri topologi ring melingkar tertutup yang isinya sebuah *node-node*, sederhana dalam *layout, signal* akan mengalir satu arah dan dapat menghindarkan

terjadinya tabrakan.

Jadi, setiap *workstation* akan menerima informasi dari satu perangkat ke perangkat lain. Kelebihan dari topologi ring adalah tidak akan terjadi *collision* atau tabrakan antar data. Sedangkan, kekurangan dari topologi ini adalah jika salah satu *node* mengalami permasalahan, maka keseluruhan jaringan akan mengalami gangguan.



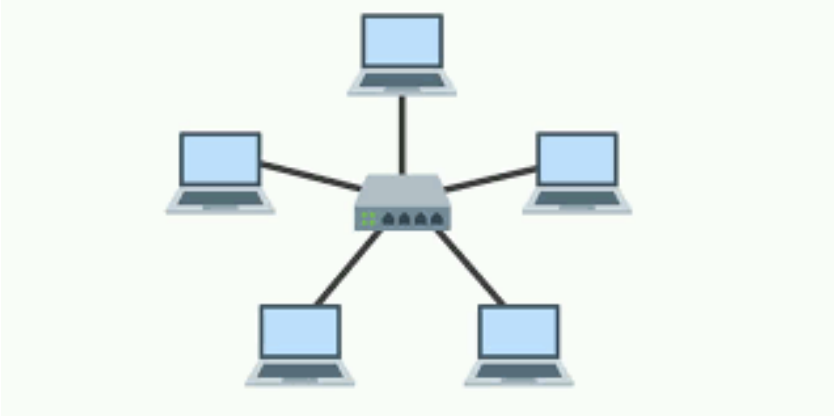
Gambar 2.2 Topologi Ring

2.2.3.3 Topologi Star

Topologi ini banyak digunakan untuk membuat suatu jaringan, memiliki kemudahan dalam memasang, melepas perngkat tambahan, serta mencari kerusakan jaringan yang ada. Sifat topologi star setiap petrangkat terhubung lurus dengan pusat *node*, *traffic* data berjalan dari perangkat ke pusat *node* dan kembali lagi, gampang untuk dikembangkan dikarenakan setiap *node* langsung tersambung ke pusat *node*, keuntungan jika terdapat suatu perangkat yang terputus, koneksi yang lain tidak akan terganggu.

Topologi star atau bintang merupakan topologi yang masing – masing *workstation* memiliki jalur yang terhubung langsung melalui *server* atau *hub*. Kelebihan dari topologi ini, adalah jika salah satu *workstation* mengalami gangguan, maka

tidak semua jaringan akan mengalami hal yang sama. Dikarenakan, setiap *workstation* memiliki jalur atau kabel sendiri. Kelemahan dari topologi star adalah membutuhkan biaya yang besar, karena membutuhkan sumber daya kabel yang banyak.

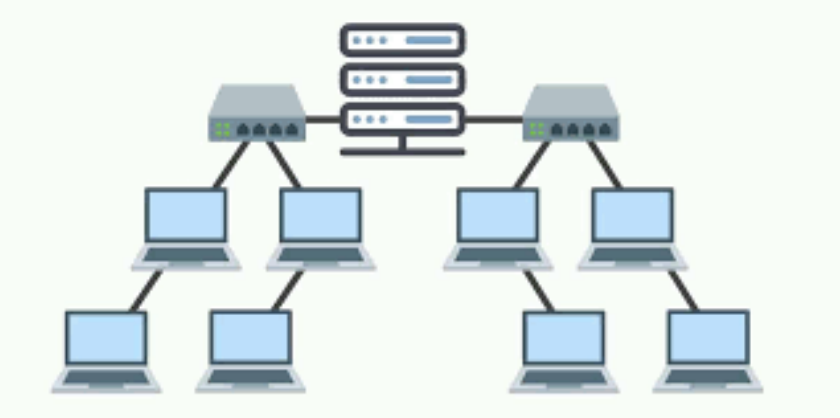


Gambar 2.3 Topologi Star

2.2.3.4 Topologi Tree

Topologi tree adalah topologi gabungan dimana antara topologi star dan bus. Topologi ini cocok diterapkan pada jaringan skala besar. Setiap penambahan perangkat pada bawah hub pusat akan dilakukan dengan mudah.

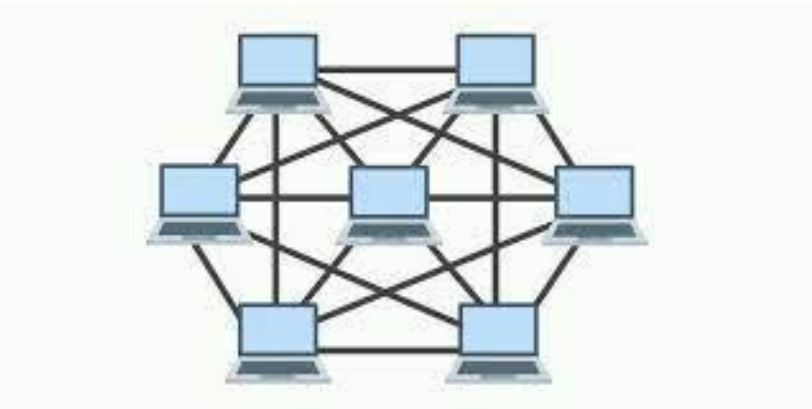
Topologi tree merupakan gabungan dari topologi star dan bus. Topologi jaringan ini menyerupai bentuk akar pohon, yang dapat dibilang hanya perangkat hub saja yang terhubung langsung menuju bus pohon. Dan setiap hub berfungsi sebagai akar dari pohon. Kelebihan dan kekurangan dari topologi tree sama dengan topologi bus dan star. Namun, dengan menggunakan jaringan pohon ini (*hybrid*), mendukung adanya perluasan jaringan yang lebih baik.



Gambar 2.4 Topologi Tree

2.2.3.5 Topologi Mesh

Topologi mesh sering dipakai ketika terdapat suatu kondisi dimana tidak adanya hubungan komunikasi yang terputus secara absolut antar *node* dalam sebuah jaringan komputer. Antar perangkat akan terhubung secara langsung selama masih dalam jaringan yang sama. Kelebihan dari topologi mesh adalah komunikasi antar komputer yang lebih cepat, serta keamanan yang lebih terjamin. Kekurangan dari topologi mesh adalah memerlukan biaya yang lebih besar dalam penyediaan kabel.[3]



Gambar 2.5 Topologi Mesh

2.2.4 *De-Militirized Zone*

De-Militarized Zone (DMZ) adalah media yang menjadi pemisah *Local Area Network* dari internet *public*. Bisa disebut juga semacam *interface* yang diletakan di tengah area internal serta eksternal dari jaringan, berfungsi memberi prmisah fisik anatara internal dan eskternal jaringan didukung oleh sistem konektivitas pada *firewall*. Kegunaan isolasi fisik *De-Militarized Zone* ini sangat berguna, dimana isolasi ini berpearan hanya untuk memberi izin akses layanan *public network* menuju ke *server* yang telah dipisahkan dan tidak diarahkan menuju *internal network.*

Dalam perancangannya, terdapat beberapa cara yang dapat digunakan untuk merancang arsitektur DMZ. Namun secara general, terdapat 2 konfigurasi desain artsitektur yang sering digunakan oleh perancang jaringan sekuritas secara umum yaitu *single firewall* dan *dual firewall*.

- ***Single Firewall***

Single firewall adalah desain konfigurasi DMZ yang menggunakan *firewall* tunggal dalam jaringan sekuritas yang dibangun. Pada konfigurasi ini, maka arsitektur sekuritas membutuhkan lebih dari 3 *interface* jaringan. Hal tersebut dikarenakan jaringan harus memenuhi 3 fungsi yaitu jaringan eksternal sebagai penghubung *firewall* dengan internet, membentuk internal *network*, dan penghubung DMZ.

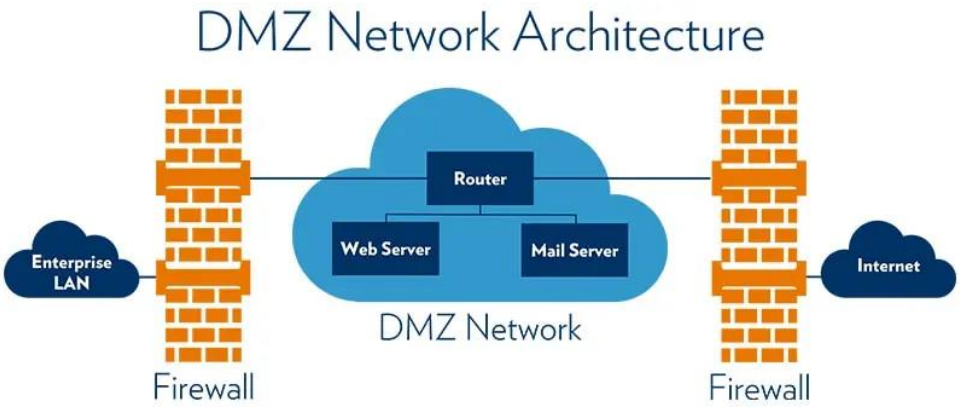
- ***Dual Firewall***

Dual firewall adalah desain konfigurasi DMZ yang sering digunakan karena memiliki level keamanan yang lebih baik dibandingkan *single firewall*. Pada konfiurasi ini, maka *firewall* yang digunakan ada 2 *firewall* yaitu *firewall* yang memberikan perizinan akses trafik eksternal menuju jaringan DMZ, dan juga *firewall* yang membatasi jaringan DMZ ke jaringan inernal. Dengan konfigurasi ini, maka peretas bukan hanya harus melewati satu *firewall*, tetapi dua *firewall* sehingga memperketat kembali otorisasi *local network* yang cenderung dilindungi.

Tujuan DMZ adalah untuk memberikan lapisan sekuritas tambahan pada jaringan *local area network* perusahaan. Sementara sisa jaringan organisasi aman di belakang *firewall*, node jaringan yang dilindungi dan dipantau menghadap ke luar jaringan internal dapat mengakses apa yang dapat diakses di DMZ. Dalam implementasinya, penggunaan DMZ dilakukan untuk memenuhi fungsi sebagai berikut:

- Menyederhanakan kegiatan pencatatan serta memantau aktivitas-aktivitas terkait pengguna yang berfokus pada penyaringan konten web.
- Mengurangi persyaratan akses bandwidth Internet guna menghindari beberapa konten di web yang dapat di-*cache* oleh *server proxy*.
- Memberikan aksesabilitas terhadap pengguna internal agar dapat menggunakan *server proxy* ketika ingin mengakses Internet.
- Memberikan proteksi ekstra terhadap data penting perusahaan

DMZ sebagai *sub network* yang terpisahkan dari *sub network* internalnya, maka terdapat beberapa layanan yang tersedia. Layanan umum yang sering ada dalam DMZ adalah *web server, mail server, FTP Server*, dan *VoIP Server*. Adanya *web server* pada DMZ, memungkinkan pengguna dapat berkomunikasi dengan database internal meskipun beberapa informasi tidak dapat diakses oleh pihak luar. *Mail server*, memungkinkan pesan yang keluar masuk dari penggunanya tersimpan dalam database secara aman. Aman dalam arti, meskipun menggunakan internet, pesan 3000v tersebut tidak dapat diakses oleh pihak luar. Akan tetapi dengan hadirnya mail server pada DMZ, hal tersebut memungkinkan pengguna masih bisa mengakses dan memanfaatkan mail server yang terhubung dengan internet.[19].

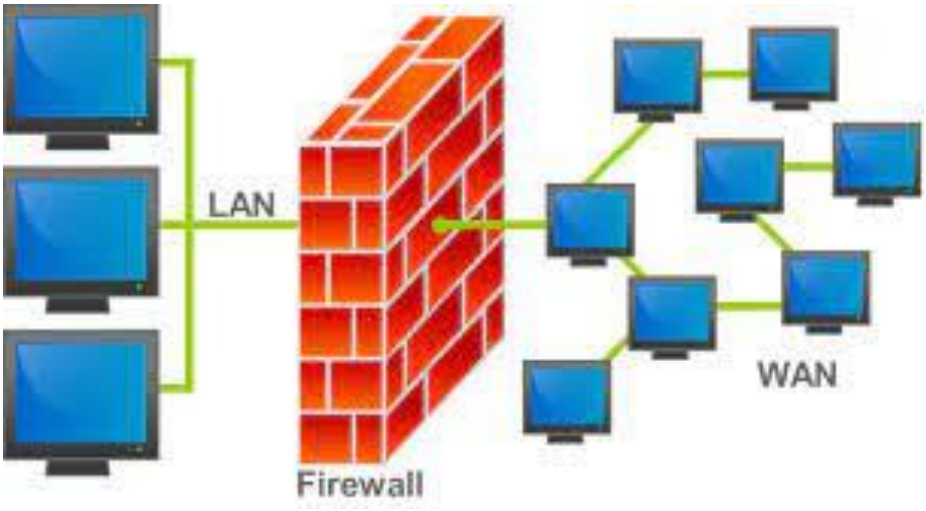


Gambar 2.6 DMZ

2.2.5 *Firewall*

Firewall merupakan suatu sistem atau perangkat lunak untuk mengizinkan koneksi aliran jaringan yang dipastikan aman untuk dapat dilintasi dan mencegah koneksi jaringan ketika dianggap tidak aman. Asalnya sebuah *Firewall* dipasang di *router* yang melintas pada *gateway* antara jaringan local dengan jaringan internet

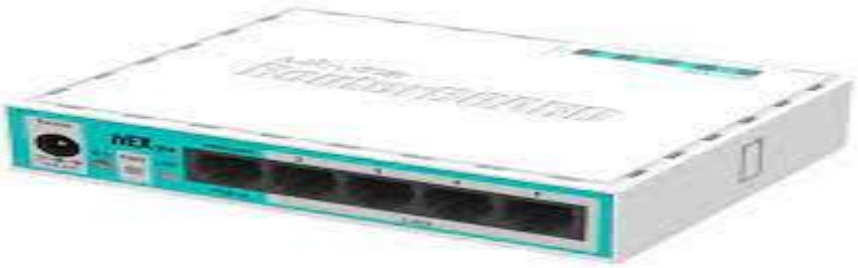
Firewall merupakan suatu komposisi yang membatasi akses antara suatu jaringan dan internet, dan jaringan yang lainnya. Firewall berfungsi guna memberi keamanan di dunia maya baik anatara lain jaringan komputer ataupun keamanan yang diserang berbagai ancaman dari internal ataupun eksternal. Dengan sebuah konfigurasi yang baik pada *firewall* maka dimungkinkan untuk memberi keamanan pada data atau komputer yang ada di jaringan tersebut supaya menjadi lebih terlindungi [20].



Gambar 2.7 Firewall

2.2.6 Mikrotik

Mikrotik merupakan sebuah system operasi atau perangkat lunak yang mampu mengubah komputer personal menjadi sebuah *router* untuk jaringan. Mikrotik awalnya digunakan oleh perusahaan penyedia layanan internet untuk ditujukan secara nirkabel kepada end user agar dapat menikmati layanan internet. Mikrotik tergolong sebagai merk dagang yang pada dasarnya merupakan *system* operasi *linux* yang fungsinya sebagai *router*. Dengan Teknik ini maka mikrotik *release* ke pasar tidak hanya *system* operasi dan *software* melainkan juga *hardware*. Sehingga saat ini mikrotik yang digunakan oleh *end user* berwujud *hardware* dan *software*[19].



Gambar 2.8 Mikrotik

2.2.7 *Quality Of Service*

Quality of Service (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan *bandwidth*, mengatasi *jitter* dan *delay*. Parameter *QoS* adalah *latency, jitter, packet loss, throughput, MOS, echo cancellation* dan *PDD. QoS* sangat ditentukan oleh kualitas jaringan yang digunakan. Terdapat beberapa faktor yang dapat menurunkan nilai *QoS*, seperti : Redaman, Distorsi, dan *Noise*. *QoS* didesain untuk membantu *end user* (klien) menjadi lebih produktif dengan memastikan bahwa *user* mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. *QoS* mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda.

Kemampuan *QoS* mengacu padae tingkat kecepatan dan kehandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. Kemapuannya merupakan kumpulan dari beberapa parameter besaran teknis, yaitu :

a). *Throughput,* yaitu kecepatan (*rate*) transfer data efektif, yang diukur dalam bps. Troughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

b). *Delay* merupakan total waktu yang dilalui suatu paket dari pengirim ke penerima melalui jaringan. *Delay* dari pengirim ke penerima pada dasarnya tersusun atas *hardware latency*, *delay* akses, dan *delay* transmisi. Delay yang paling sering dialami oleh trafik yang lewat adalah *delay* transmisi. Untuk aplikasi-aplikasi suara dan video interaktif, kemunculan dari *delay* akan mengakibatkan sistem seperti tak merespon.

c). *Jitter* merupakan variasi dari *delay end-to-end*. Level-level yang tinggi pada *jitter* dalam aplikasi-aplikasi berbasis *UDP* merupakan situasi yang tidak dapat diterima dimana aplikasi-aplikasinya merupakan aplikasi-aplikasi *real-time*, seperti sinyal audio dan video. Pada kasus seperti itu, *Jitter* akan menyebabkan sinyal terdistorsi, yang dapat

diperbaiki hanya dengan meningkatkan *buffer* di antrian.

2.2.8 *VirtualBox*

VirtualBox adalah perangkat lunak pada sistem operasi virtualisasi yang mampu mengubah sesuatu menjadi sebuah bentuk nyata. Contoh jika akan melakukan instalasi operasi windows pada PC, maka secara tidak langsung dapat mengoperasikan sistem operasi lainnya di *windows*. Dengan demikian, akan memudahkan pengguna dalam belajar menginstall sistem pada operasi. Cukup dengan menggunakan *VirtualBox*, maka dapat mengunduh *linux* di *windows*. Ada beberapa keuntungan menggunakan aplikasi *VirtualBox*, yaitu:

a) Keuntungan Penggunaan *Virtualbox*

   Keuntungan menggunakan *VirtualBox* adalah aplikasi yang bisa diunduh secara gratis pada sebuah situs resmi *Oracle VM VirtualBox*. Selain itu, aplikasi ini selalu upgrade dan tentunya bisa beroperasi menggunakan dua sistem secara bersama pada satu PC.

b) Mudah Dalam Belajar Komputer

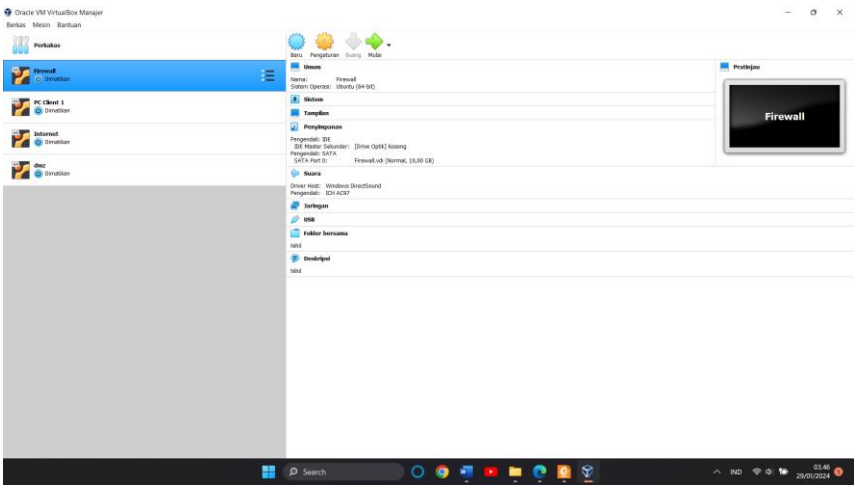
   VirtualBox sangat memudahkan pengguna dalam hal mempelajari komputer, tidak perlu khawatir PC akan alami kerusakan. Sebab semua permasalahan dapat diatasi dengan menggunakan *VirtualBox*. Apalagi dengan adanya perangkat lunak tersebut, maka semua komputer *windows* dapat beroperasi dengan lancar pada PC 32 bit atau 64 bit.

c) Konfigurasi Penginstalan Cukup Mudah

   VirtualBox termasuk kedalam teknologi *hosted hypervisor*, dimana sebuah virtualisasi yang bisa diinstal menggunakan pengoperasian sistem pada *host*. *Oracle* merupakan perusahaan yang mengembangkan *VirtualBox* sebagai *open source*, yang bisa digunakan dalam penginstalan sistem *Linux, Solaris, Macintosh* dan *Windows*. Lalu dengan adanya dukungan tiga macam virtual *hardisk drive(VDI, VMDK* dan *VHD*) inilah yang memudahkan aktivitas dalam melakukan ekspor dan impor pada *software*.

d) Hemat Tarif Investasi Untuk Hardware

Dengan adanya perangkat tersebut, maka pengguna tidak harus mengadopsi perangkat untuk komputer. Sebab pengguna dapat menjalankan sebuah sistem lain dalam satu layar. Adanya perangkat tersebut dinilai mampu untuk menghemat tarif hardware dan tidak perlu untuk meminang hardware baru. Kapasitas pada komputer pun dapat disesuaikan dengan adanya *harddisk host*.

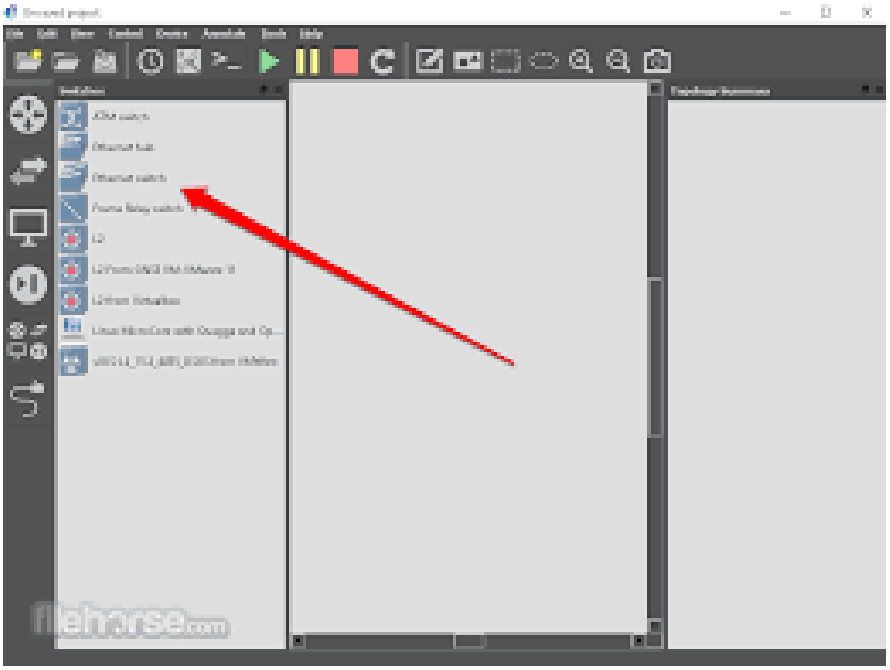


Gambar 2.9 *VirtualBox*

2.2.9 *Graphic Network Simulator (GNS3*)

Graphic Network Simulator (GNS3) adalah sebuah perangkat lunak yang bersifat *open source* (GNU GPL) yang digunakan untuk simulasi teknologi jaringan komputer. Kemampuan simulasi yang diberikan GNS3 tidak hanya kemampuan simulasi sederhana namun dapat memberikan gambaran tentang cara kerja jaringan yang mendekati nyata. GNS3 juga dapat digunakan untuk simulasi jaringan yang cukup kompleks yang dapat dibuat dengan mudah oleh *network administrator* dengan fitur *plug and play*. GNS3 memiliki fitur *plug and play* dengan antar muka yang mudah dan menarik untuk perancangan jaringan komputer. GNS3 mampu berjalan di beberapa *system* operasi antara lain Windows, Linux, dan Mac OS X. GNS3 disebut sebagai simulator yang cukup mudah digunakan dan memiliki basis GUI dan

rilis tahun 2008. Dengan GNS3 maka *network administrator* dapat melakukan simulasi dan virtualisasi rancangan jaringan yang mirip dengan kondisi nyata.



Gambar 2.10 GNS3