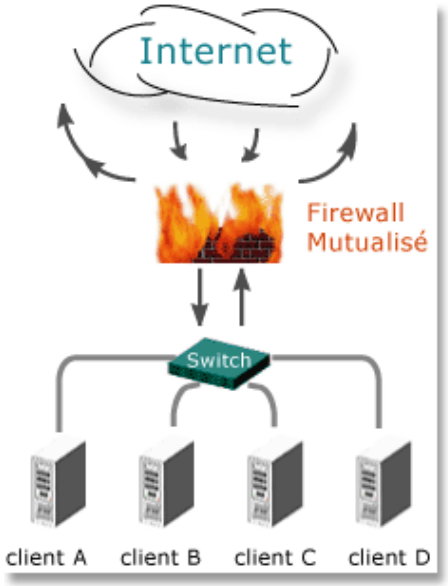
Firewall

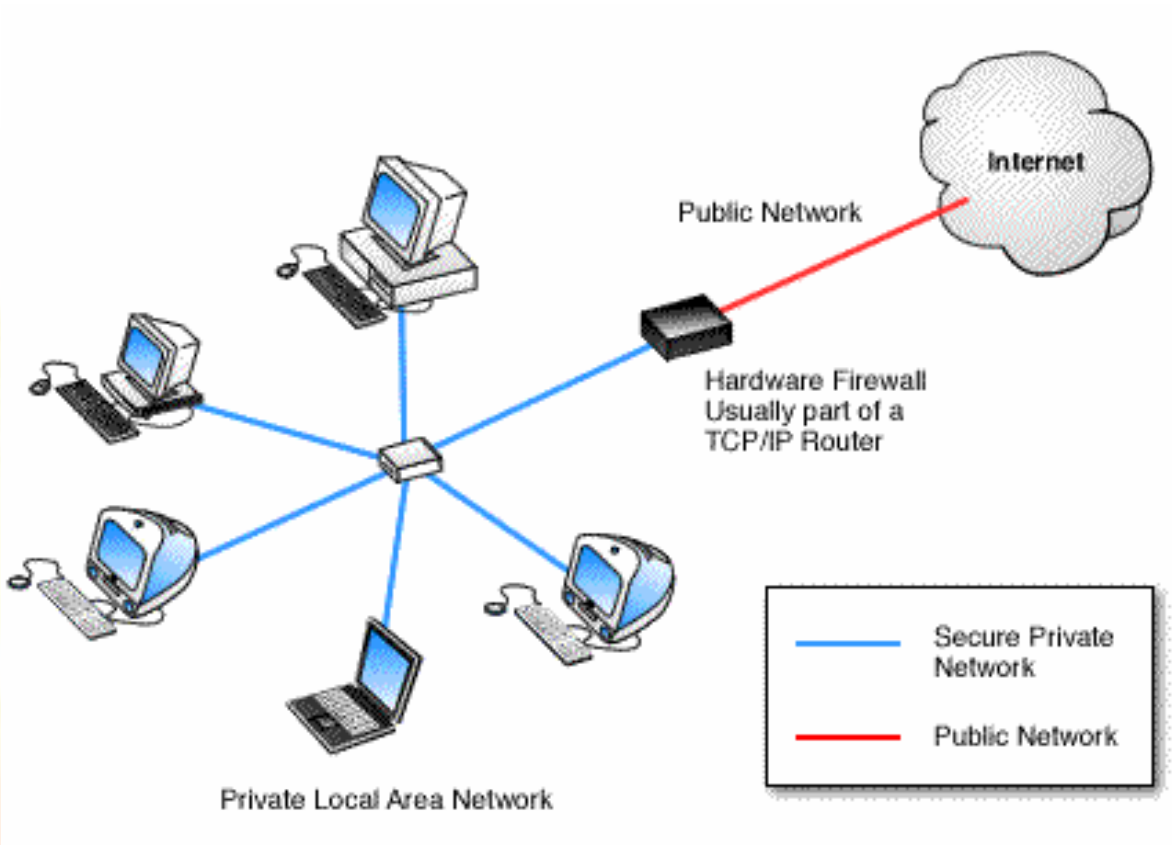
Definisi Firewall

Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini. Tujuan adanya firewall adalah untuk menjaga (*prevent) agar akses (ke dalam maupun ke luar)* dari orang yang tidak berwenang (*unauthorized access) tidak dapat dilakukan.* Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy) dari organisasi yang* bersangkutan, yang dapat dibagi menjadi dua jenis:

- ***prohibitted***
- ***permitted***

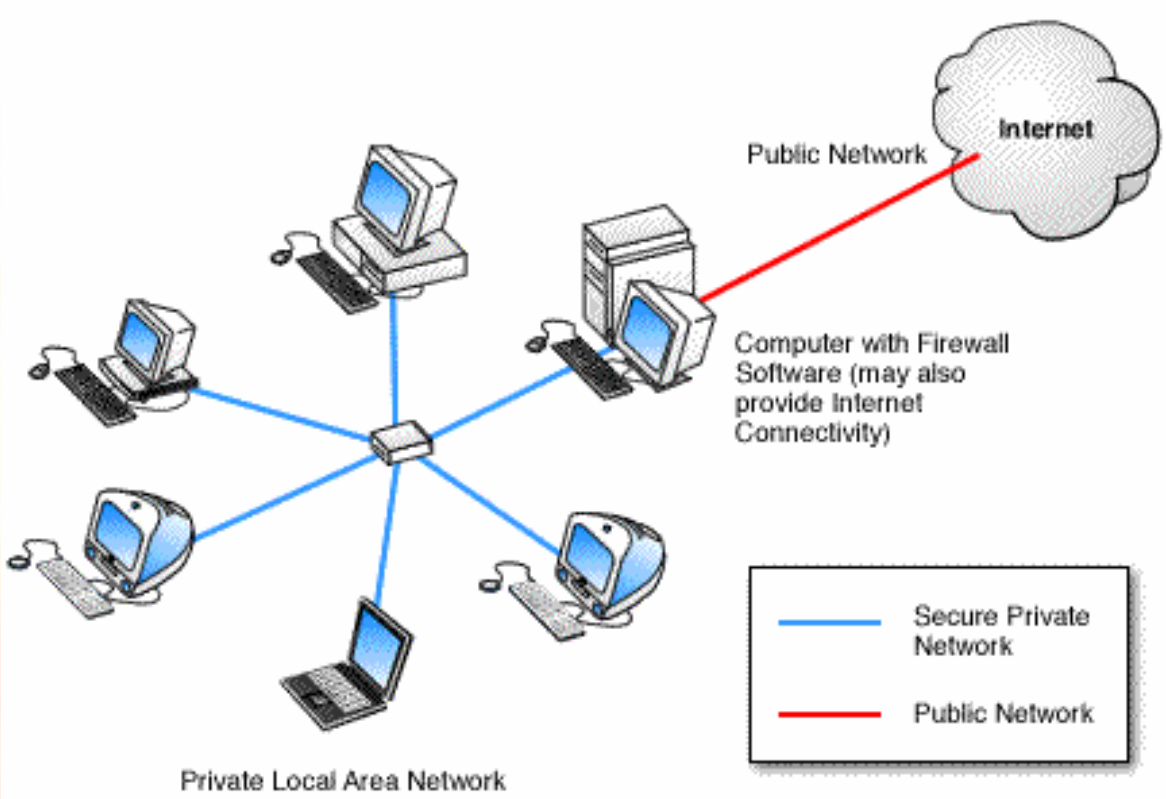


Gambar 1: Hardware Firewall: Hardware firewall menyediakan perlindungan ke Local Area Network



Gambar 2: Komputer dengan Firewall Software

Komputer yang menggunakan firewall software untuk proteksi jaringan



Secara konseptual terdapat 2 macam firewall:

1. *Network Level*

mendasarkan keputusan pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP.

2. *Application Firewall*

Host yang berjalan sebagai proxy server, yang tidak mengijinkan lalulintas antar jaringan dan melakukan *logging dan auditing lalulintas yang melaluinya.*

• Firewall bekerja dengan mengamati paket IP (Internet Protocol) yang melewatinya. Berdasarkan konfigurasi dari firewall maka akses dapat diatur berdasarkan IP address, port, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing firewall.

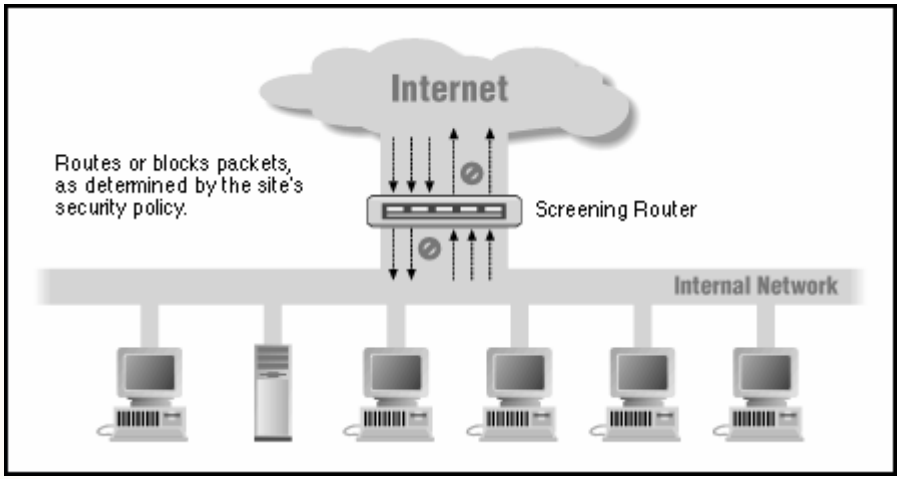
• Firewall dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai (administrator) tinggal melakukan konfigurasi dari firewall tersebut.

• Firewall juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah server (baik UNIX maupun Windows NT), yang dikonfigurasi menjadi firewall.

Untuk menjaga fungsi komunikasi jaringan dalam lingkungan yang berfirewall, dilakukan dua cara :

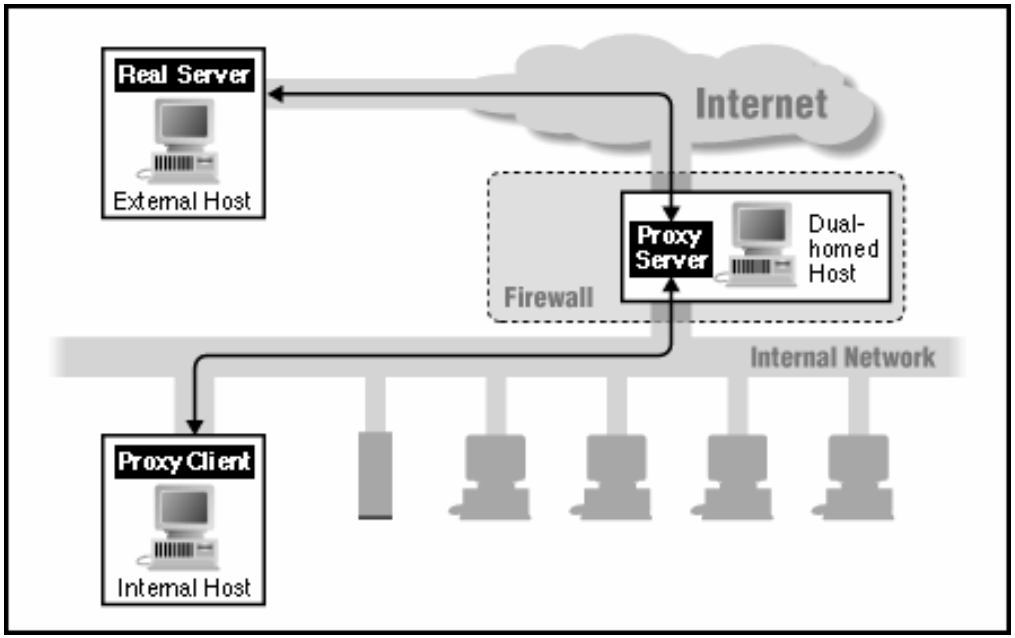
1. **Packet filtering**

mekanisme pengontrolan data yang diperbolehkan mengalir dari dan atau ke jaringan internal dengan menggunakan beberapa paremeter yang tercantum dalam header paket data: arah (inbound atau outbond), address asal dan tujuan, port asal dan tujuan serta jenis protokol transport. Seperti telnet dan SMTP (Single Mail Transport Protocol).



2. Menggunakan sistem proxy

dimana setiap komunikasi yang terjadi antar kedua jaringan harus dilakukan melalui suatu operator, dalam hal ini proxy server. Protokol FTP (File Transport Protocol) lebih efektif ditangani dengan sistem Proxy. Kebanyakan firewall menggunakan kombinasi kedua teknik ini (Packet filtering dan Proxy)



Beberapa perangkat lunak berbasis UNIX yang dapat digunakan untuk melakukan IP filtering antara lain:

- **ipfwadm:**

merupakan standar dari sistem Linux yang dapat diaktifkan pada level kernel

- **ipchains:** versi baru dari Linux kernel packet filtering yang diharapkan dapat menggantikan fungsi ipfwadm.

Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya.

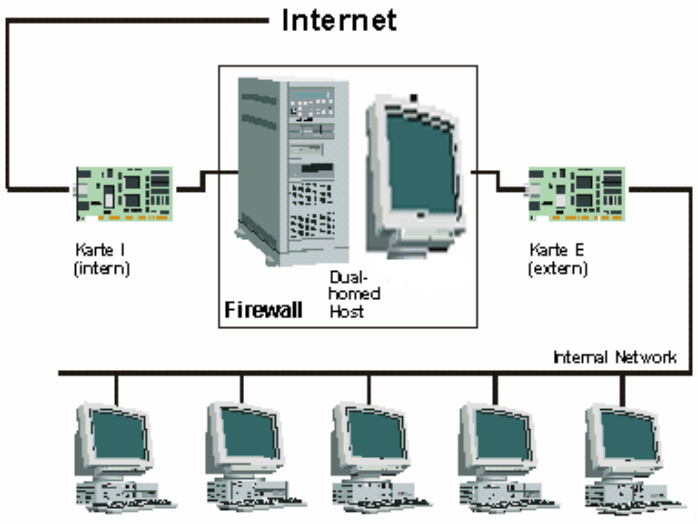
Di sisi client sering kali dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS. Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain:

- ***Socks: proxy server oleh NEC Network Systems Labs***
- ***Squid: web proxy server***

Arsitektur dasar Firewall

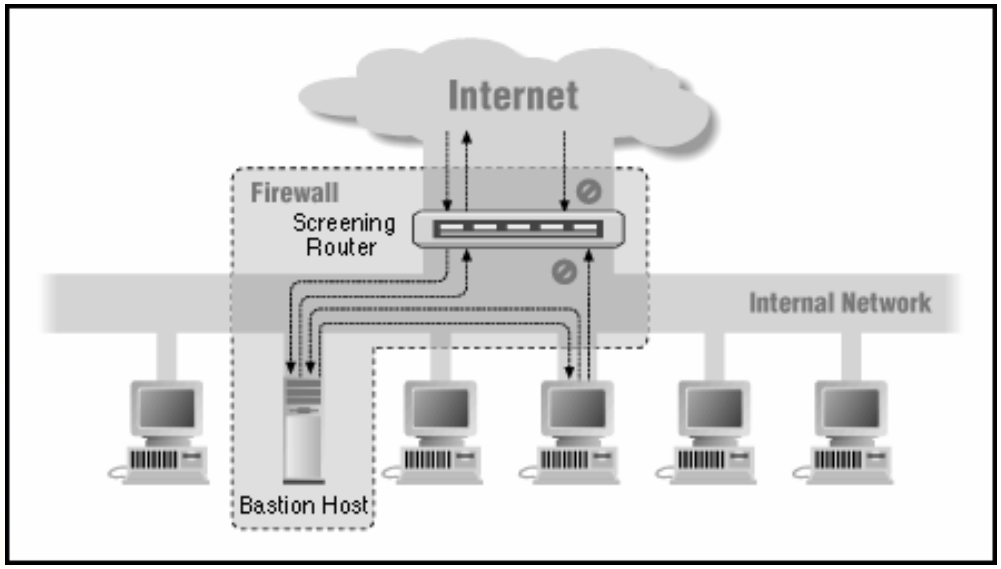
1. Arsitektur dengan dual-homed host
(*dual homed gateway/DHG)*

Menggunakan sebuah komputer dengan (minimal) dua NIC. Interface pertama dihubungkan ke jaringan internal dan yang lainnya dengan internet. *Dual homed host-nya sendiri* berfungsi sebagai *bastion host (Suatu* sistem komputer yang harus memiliki keamanan yang tinggi, karena biasanya peka terhadap serangan jaringan, Ada 3 macam arsitektur dasar firewall, yaitu : biasanya terhubung langsung ke internet dan menjadi titik utama komunikasi dengan jaringan internal.)



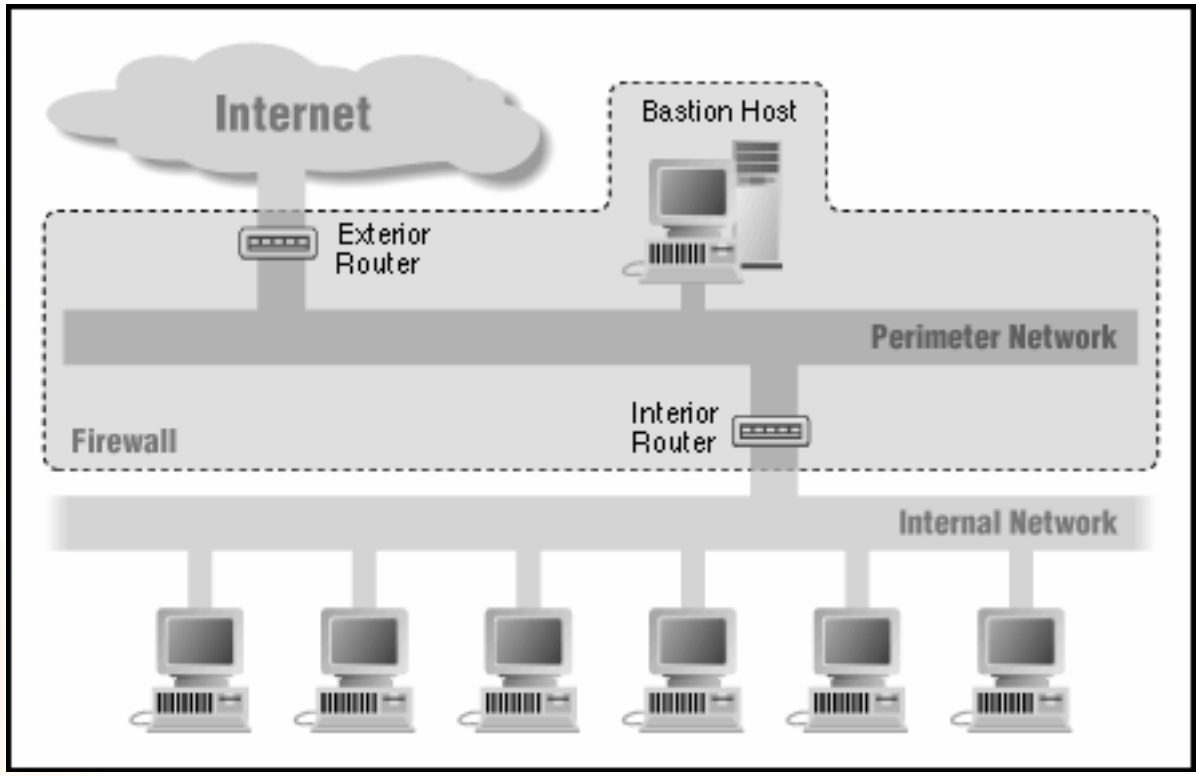
2. Screened-host (screened host gateway/SHG)

fungsi firewall dilakukan oleh sebuah screening-router dan bastian host. Router ini akan menolak semua trafik kecuali yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan.



3. Screened subnet (*screened subnet gateway (SSG)*

Firewall dengan arsitektur ini menggunakan dua Screened-router dan jaringan tengah (*perimeter network) antara* kedua router tersebut, dimana ditempatkan bastion host.



Beberapa Software Firewall

- Zone Alarm Pro Firewall
- PC Tools Firewall Plus
- Windows XP Firewall Port & Application Manager
- Norton Internet Security
- Prevx1 2.0.15 build 6

TERIMA KASIH

SOAL-SOAL LATIHAN

1. Firewall biasanya menggunakan dua teknik kombinasi untuk mengamankan jaringan yaitu menggunakan proxy dan …
   a. IPlog c. Paket Filtering b. Gateway d. Socks

2. Konfigurasi firewall tergantung pengaturan oleh administrator jaringan yang terbagi menjadi dua yaitu :
   a. Prohibitted & Permitted c. Prohibitted
   b. Adminted & Permitted d. Permitted

3. Penggunaan dua buah NIC dalam 1 PC adalah salah satu arsitektur firewall
   a. Screened-host c. Dual-homed host
   b. Screened subnet d. Host gateway

4. Penggunaan dua buah NIC dalam 1 PC adalah salah satu arsitektur firewall
   a. Screened-host c. Dual-homed host
   b. Screened subnet d. Host gateway

5. Software pada UNIX yang digunakan untuk melakukan IP filtering, yaitu …
   a. ipchains c. Samspade
   b. ipcalt d. Fwadm