



# **COMPUTER SECURITY**

**Firewall**

**Pertemuan VII**

**Rianto, S.Kom., M.Eng.**

Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : [me@rianto.com](mailto:me@rianto.com) Website : <http://www.rianto.com>

Mobile : 0815 787 02873

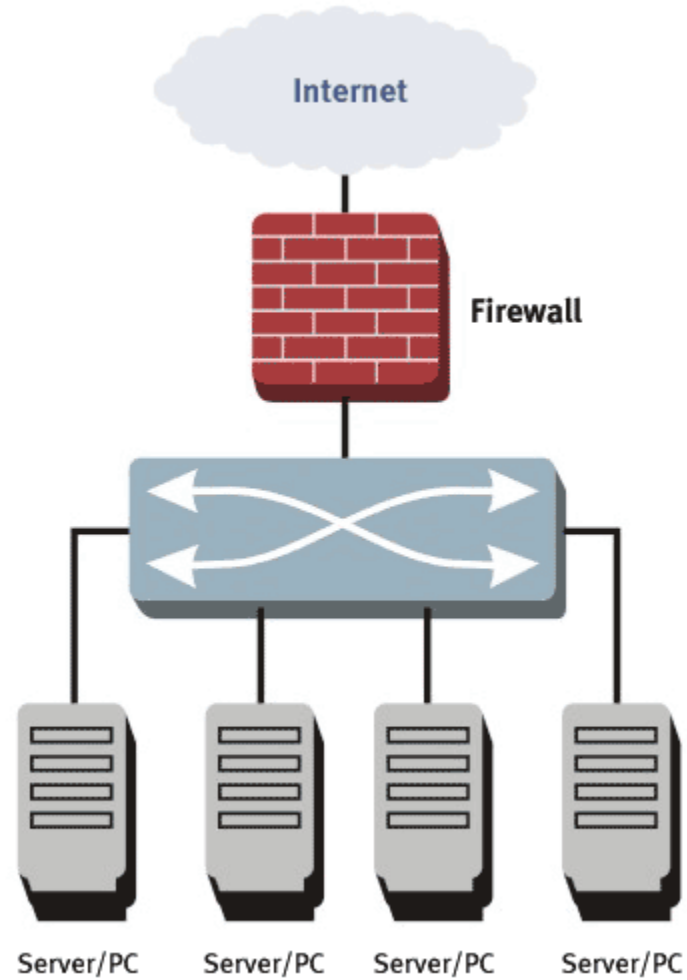
# Definisi Firewall



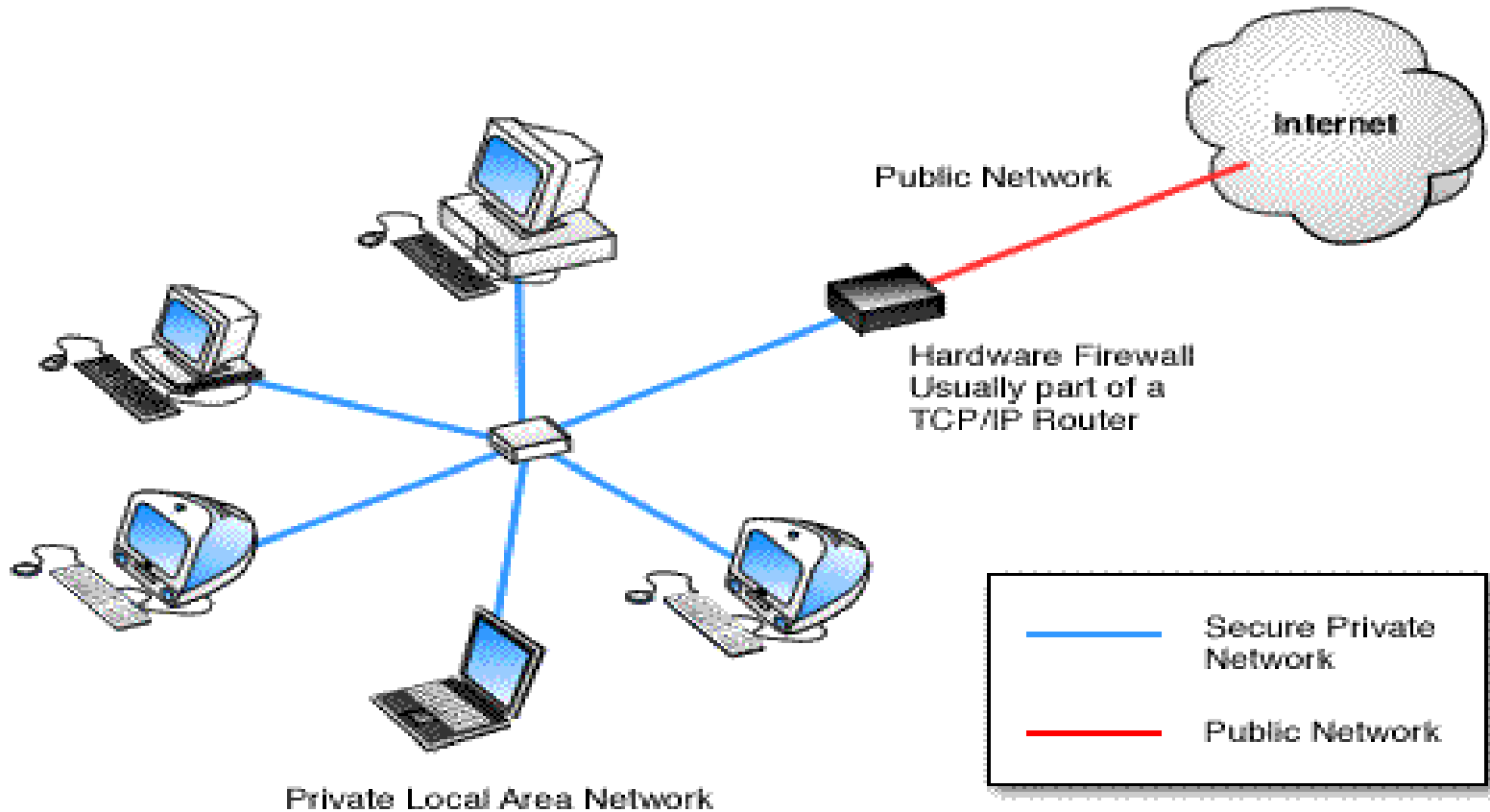
Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini.

Tujuan adanya firewall adalah untuk menjaga (*prevent*) agar akses (ke dalam maupun ke luar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan.

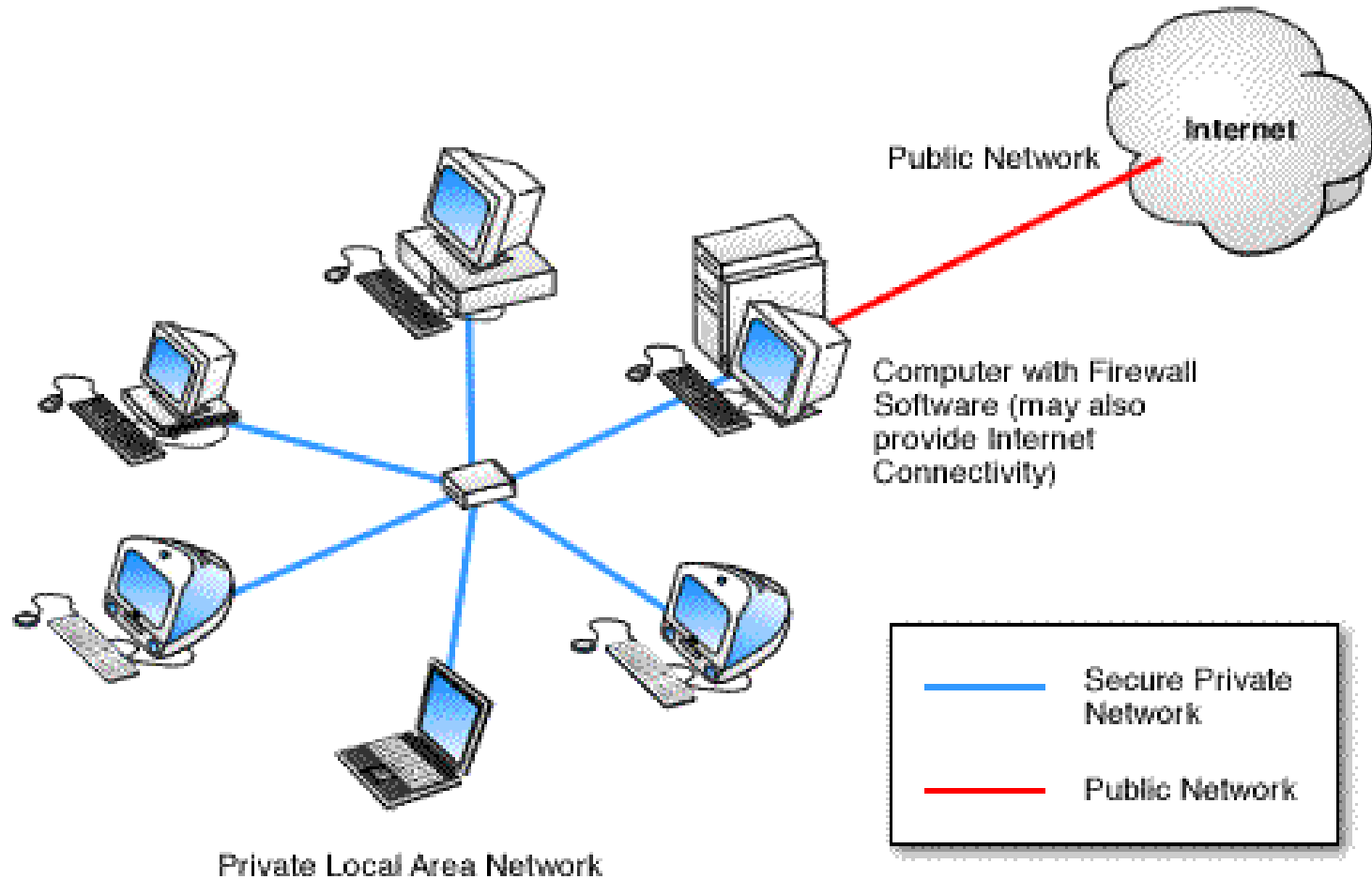
# Skema Umum Firewall



# Hardware Firewall



# Software Firewall



# Cara Kerja Firewall

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.

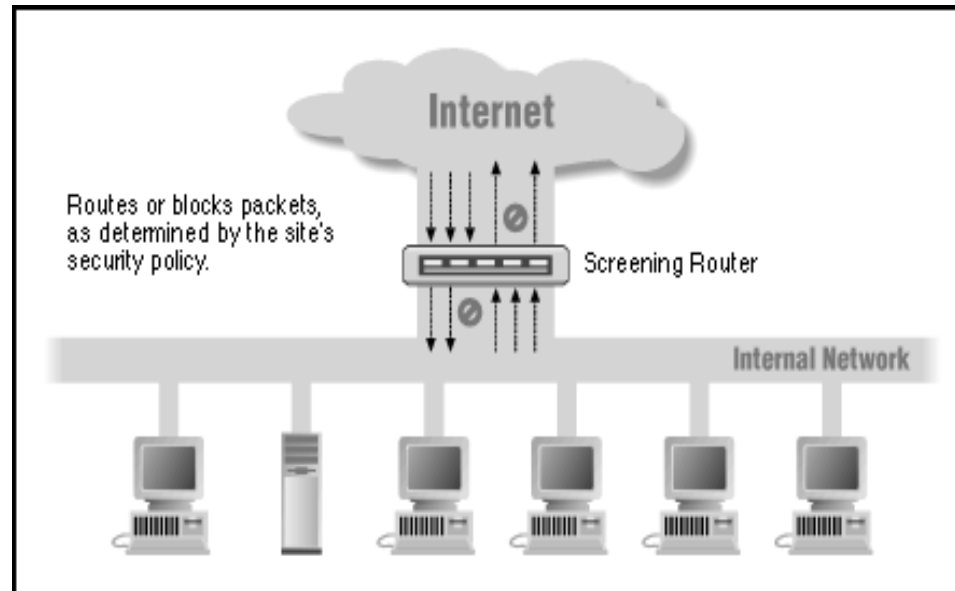
# Cara Kerja Firewall

- 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.

# Cara Komunikasi Firewall

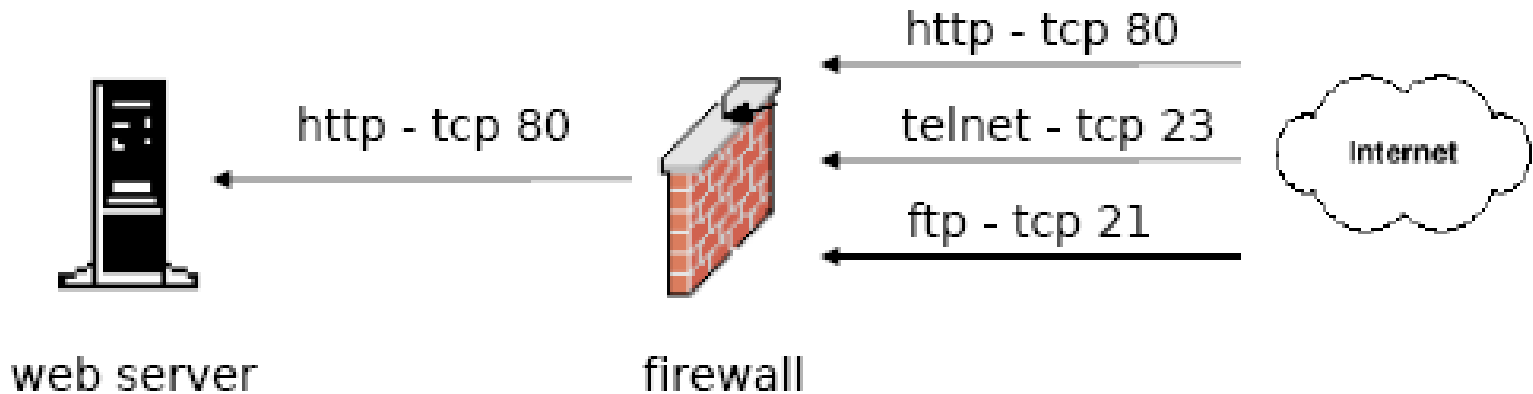
## Packet filtering

mekanisme pengontrolan data yang diperbolehkan mengalir dari dan atau ke jaringan internal dengan menggunakan beberapa parameter 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).



# Cara Komunikasi Firewall

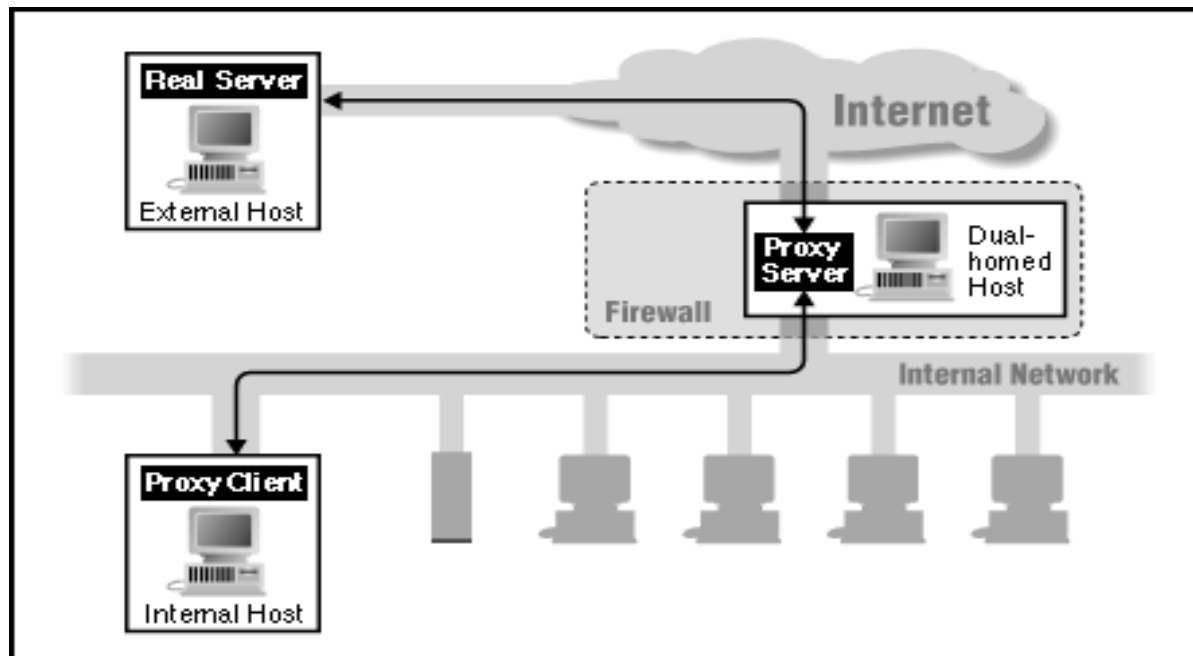
## Packet Filtering



# Cara Komunikasi Firewall

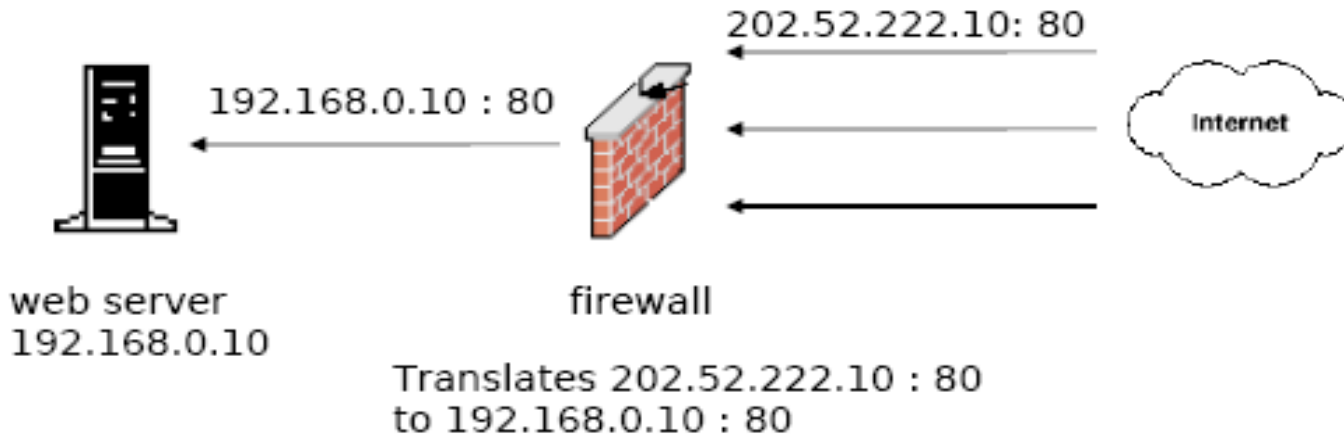
## Sistem Proxy

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)

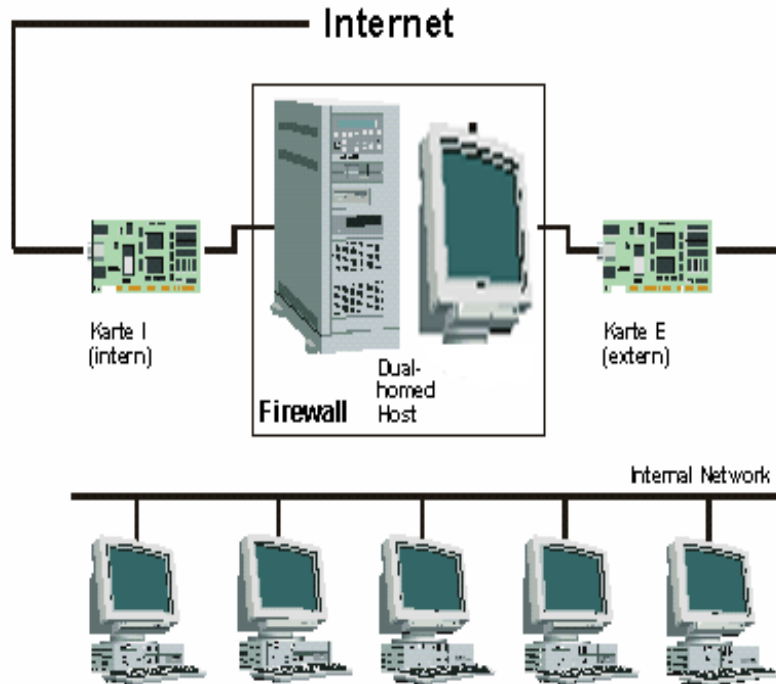


# Cara Komunikasi Firewall

## Sistem Proxy



# Arsitektur Firewall



## Dual Homed Gateway/DHG

Menggunakan sebuah komputer dengan (minimal) dua NIC. Interface pertama dihubungkan ke jaringan internal dan yang lainnya dengan internet.

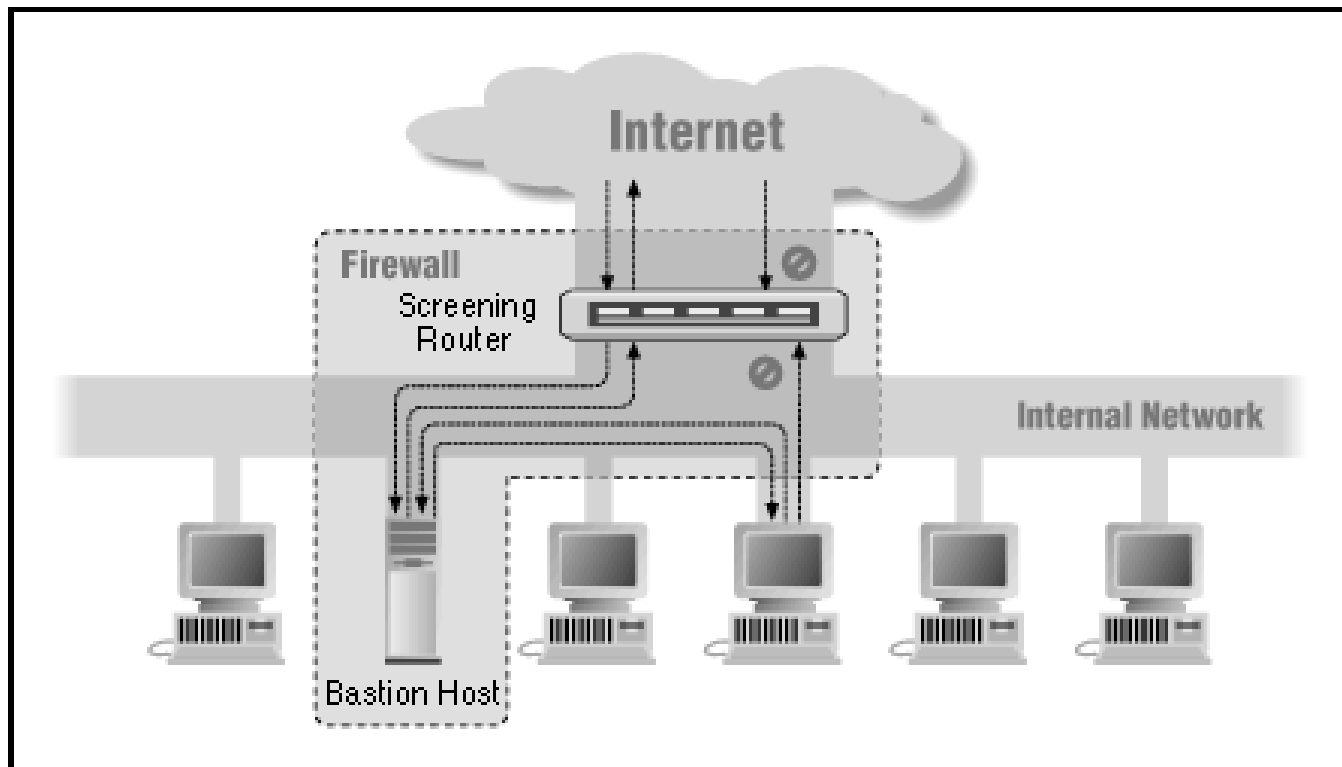
*Dual homed host*-nya sendiri berfungsi sebagai *bastion host* (Suatu sistem komputer yang harus memiliki keamanan yang tinggi, karena biasanya peka terhadap serangan jaringan,

biasanya terhubung langsung ke internet dan menjadi titik utama komunikasi dengan jaringan internal.)

# Arsitektur Firewall

## Screened-host (screened host gateway/SHG)

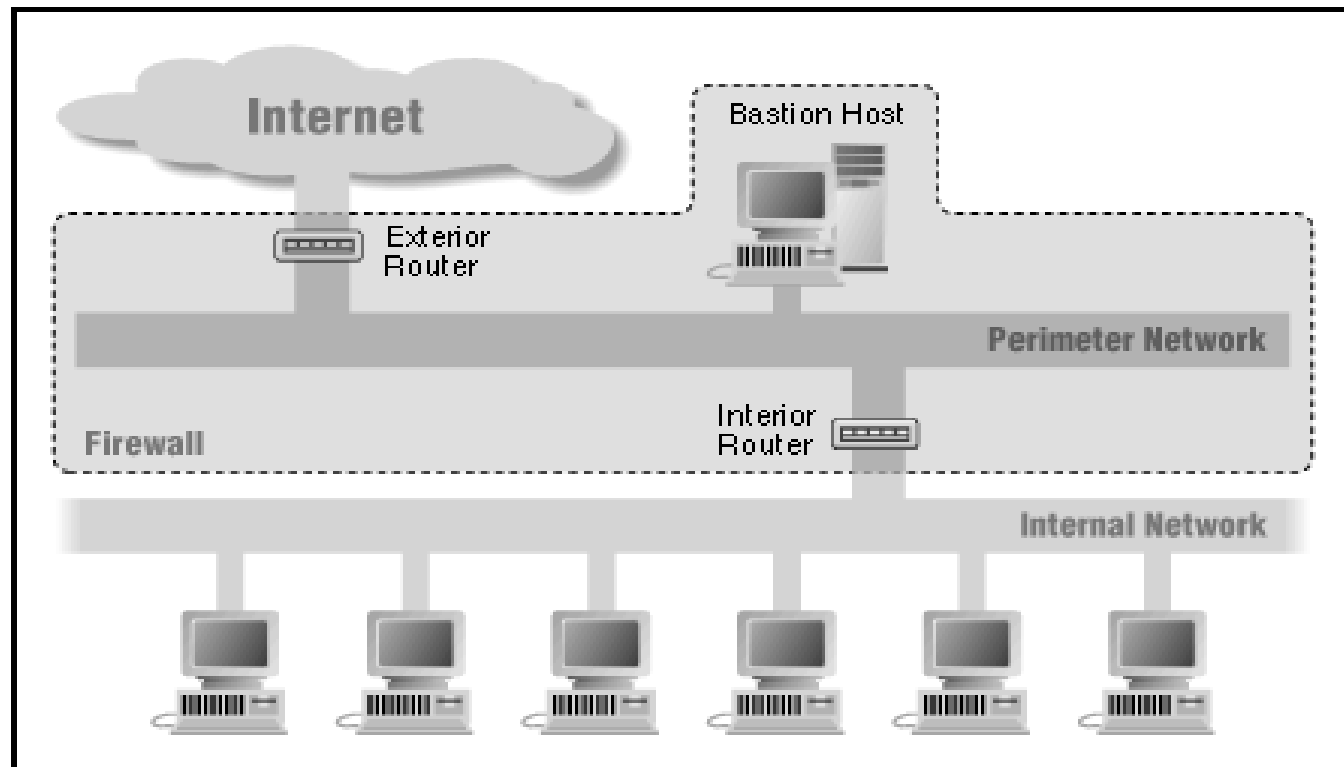
fungsi firewall dilakukan oleh sebuah screening-router dan bastian host. Router ini akan menolak semua trafik kecuali yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan.



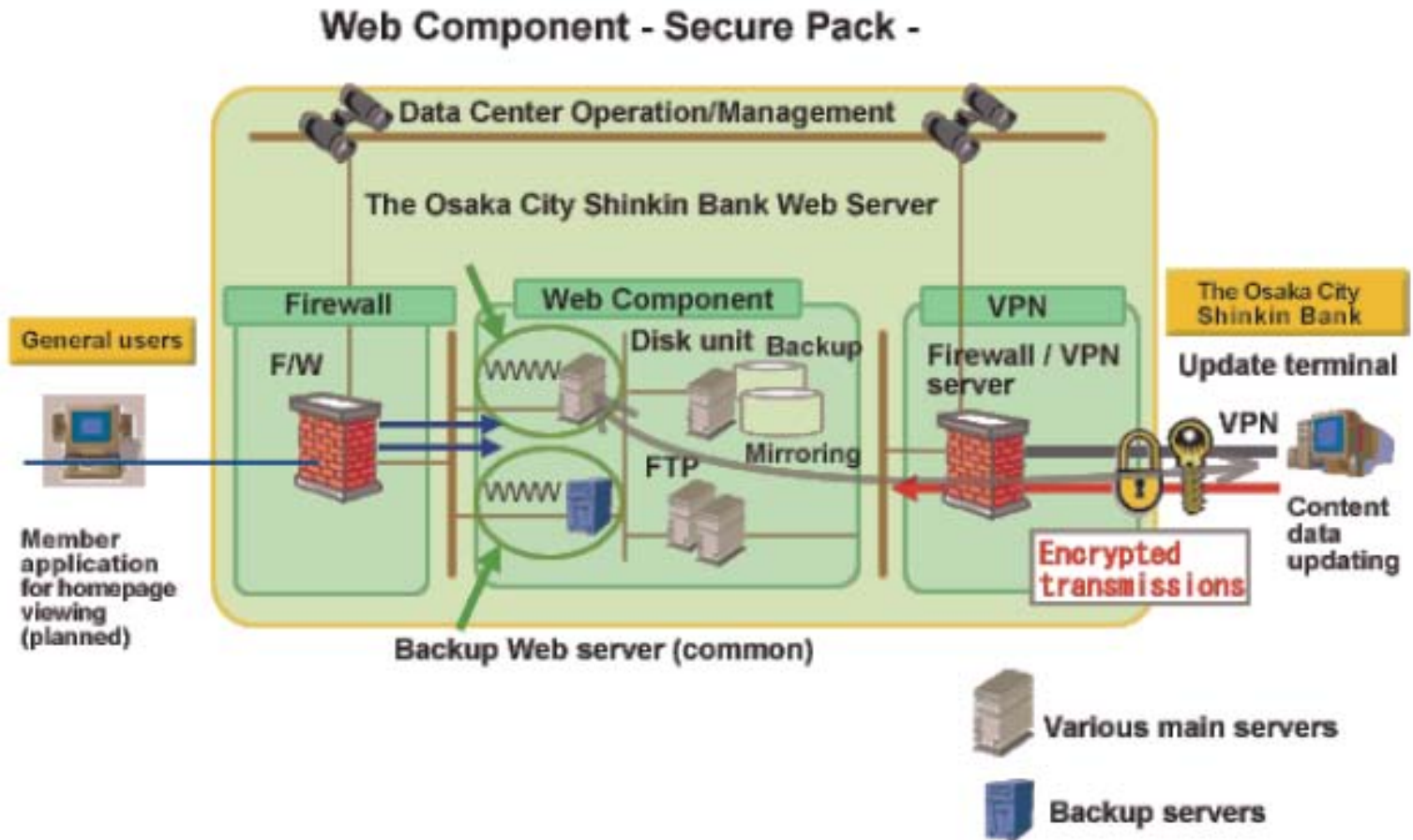
# Arsitektur Firewall

## 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.



# Contoh Implementasi Firewall



# Aplikasi

- Intrusion Detection System/Intrusion Preventing System (IDS/IPS)
  - SNORT [www.snort.org](http://www.snort.org)
  - ISS RealSecure [www.iss.net](http://www.iss.net)
  - NFR [www.nfr.com](http://www.nfr.com)
  - PortSentry [www.psionic.com](http://www.psionic.com)
- IDS yang bekerja sama dengan Firewall

# Aplikasi

## **Intrusion Detection System**

- Sistem untuk mendeteksi adanya “intrusion”/penyusupan yang dilakukan oleh “intruder”/penyusup
- Berfungsi seperti alarm
- Intrusion didefinisikan sebagai kegiatan yang bersifat *anomaly, incorrect, inappropriate* yang terjadi di jaringan atau di host

# Aplikasi

## **Jenis Intrusion Detection System**

- Networkbased (NIDS)  
memantau anomali di level jaringan, misal melihat adanya network scanning
- Hostbased (HIDS)  
memantau anomali di host, misal memonitor logfile, process, file ownership, file permission

# Aplikasi

## **Snort Intrusion Detection System**

- OpenSource (GPL)
- Berfungsi sebagai NIDS, HIDS, Packet Sniffer
- Berjalan di Unix/Linux/Windows
- Beroperasi berdasarkan “rules”