

# SISTEM KEAMANAN JARINGAN KOMPUTER

*Mata kuliah Jaringan Komputer*  
*Iskandar Ikbai, S.T., M.Kom*

# Materi :

---

- ❑ Strategi Merancang Sistem Keamanan
- ❑ Peningkatan Keamanan Jaringan
- ❑ Variasi Arsitektur Firewall
- ❑ Software Firewall

# Strategi Merancang Sistem Keamanan

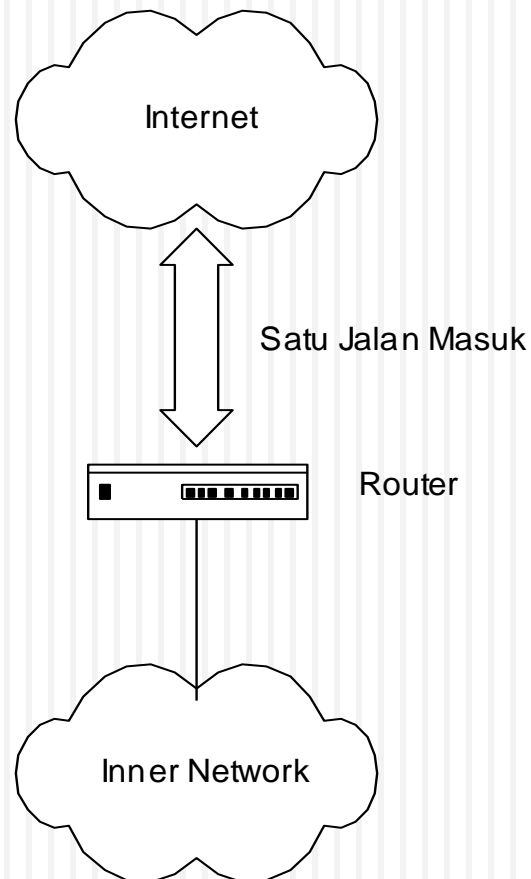
- Threat pada jaringan yang semakin beragam
  - ▣ Hacker, cracker
  - ▣ Virus, Malware
- Internet
- Tujuan Sekuriti jaringan : memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan komputer pada titik-titik yang tepat sehingga lebih efisien.

# Strategi Merancang Sistem Keamanan

- Strategi Dasar Merancang Sekuriti Jaringan
  - ▣ Hak Akses
    - User yang memiliki hak untuk mengakses sistem
  - ▣ Lapisan Sekuriti
    - Network Security
    - Host/server security
    - Human security
  - ▣ Satu jalur Masuk
    - Pengawasan terpusat
    - Jika gagal – langsung masuk dalam sistem

# Strategi Merancang Sistem Keamanan

- Strategi Dasar Merancang Sekuriti Jaringan
  - ▣ Satu jalur Masuk

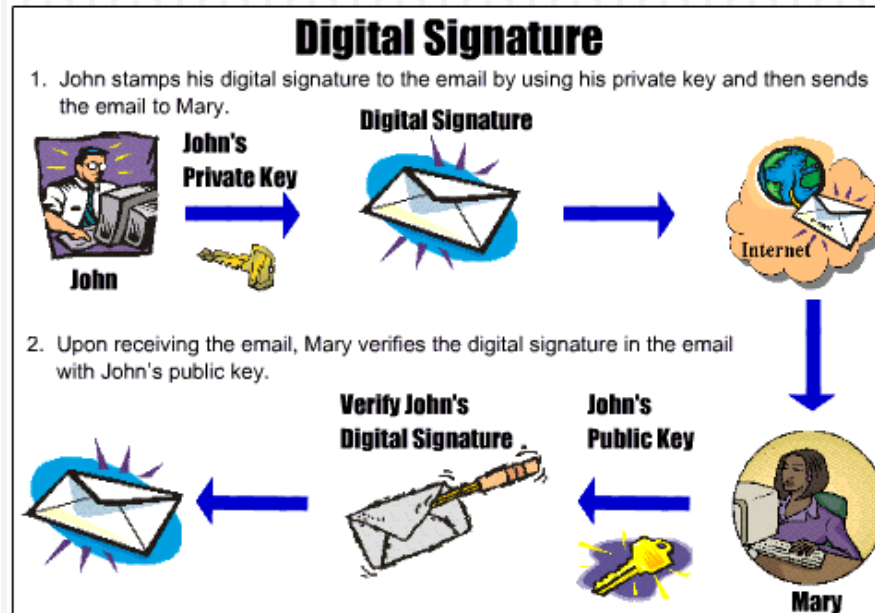


# Strategi Merancang Sistem Keamanan

## □ Strategi Dasar Merancang Sekuriti Jaringan

### ▣ Enkripsi Data Dan Digital Signature

- RSA, MD-5, IDEA, SAFER, Skipjack, Blowfish

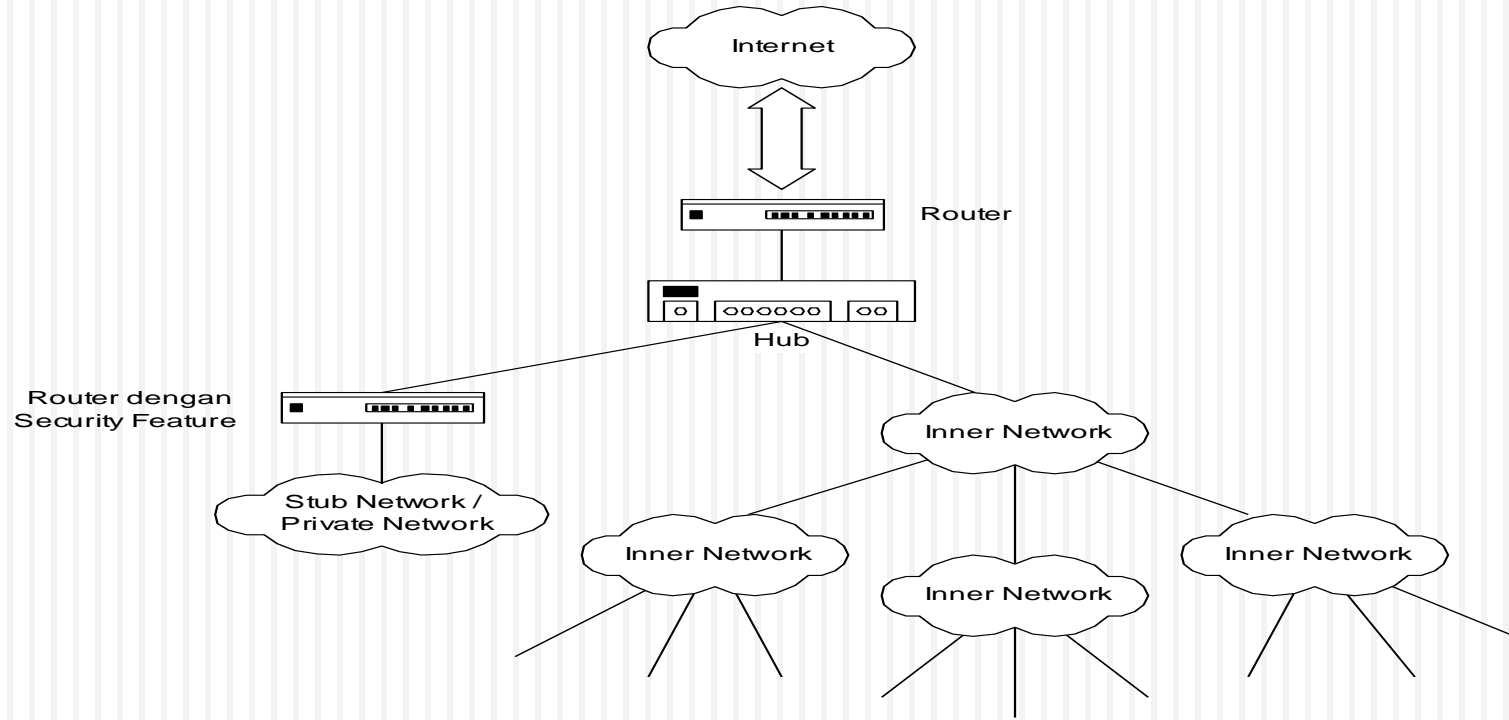


# Strategi Merancang Sistem Keamanan

## □ Strategi Dasar Merancang Sekuriti Jaringan

### ▣ Stub Sub-Network

- *Stub sub-network* adalah sub-jaringan komputer yang hanya memiliki satu jalur keluar masuk sub-jaringan tersebut. Strategi ini digunakan untuk mengisolasi sub-jaringan komputer yang benar-benar memerlukan perlindungan maksimal.



# Strategi Merancang Sistem Keamanan

- Strategi Dasar Merancang Sekuriti Jaringan
  - ▣ Cari Titik Lemah
    - Mencari titik lemah pada jaringan, dilakukan oleh administrator
  - ▣ Dua Sikap Umum
    - Prohibitive – Menolak secara umum
    - Permissive – Menerima Secara Umum
  - ▣ Keanekaragaman
    - Perangkat keras
    - Perangkat Lunak
    - Kombinasi strategi sekuriti



# Peningkatan Keamanan Jaringan

- Strategi Dasar Merancang Sekuriti Jaringan
  - ▣ Cari Titik Lemah
    - Mencari titik lemah pada jaringan, dilakukan oleh administrator
  - ▣ Dua Sikap Umum
    - Prohibitive – Menolak secara umum
    - Permissive – Menerima Secara Umum
  - ▣ Keanekaragaman
    - Perangkat keras
    - Perangkat Lunak
    - Kombinasi strategi sekuriti

# Peningkatan Keamanan Jaringan

- Semakin beragamnya ancaman
- Salah satu alternatif untuk meningkatkan keamanan jaringan komputer adalah dengan menggunakan suatu metode pengamanan jaringan yang dinamakan dengan Firewall.

# Peningkatan Keamanan Jaringan

## □ Firewall

- Definisi dasar dari Firewall sendiri adalah komponen atau satu kelompok komponen yang mengatur akses antara internal network (network yang akan dilindungi) dengan eksternal network (Internet) atau antara beberapa kumpulan network
- Firewall dapat berupa solusi hardware dan software yang membatasi akses dari jaringan internal ke internet atau sebaliknya
- Firewall dapat juga digunakan untuk memisahkan dua atau lebih bagian jaringan lokal

# Peningkatan Keamanan Jaringan

## □ Istilah-istilah dalam Firewall

### ▣ Host

- Sistem komputer yang terhubung pada suatu network

### ▣ Bastion Host

- Sistem komputer yang memiliki tingkat sekuritas yang tinggi karena sistem ini rawan terhadap serangan hacker dan cracker, karena mesin ini diekspos keluar (internet)

### ▣ Packet Filtering

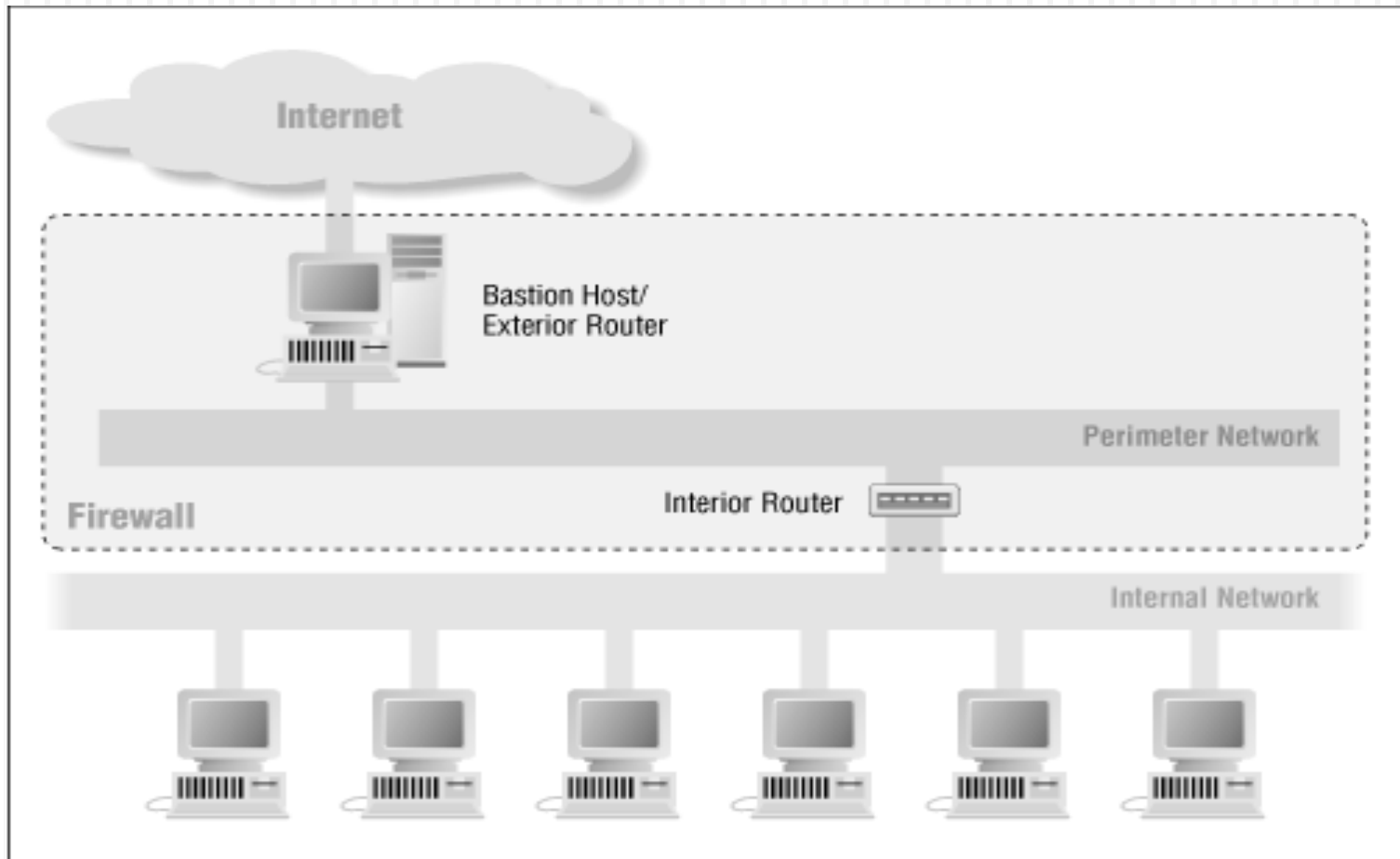
- Mengatur secara selektif alur data yang melintasi suatu network. Packet filtering bertugas melewatkan atau memblokir suatu paket data yang melintasi network

### ▣ Perimeter Network

- Network tambahan yang terdapat diantara network yang dilindungi dengan network eksternal, menyediakan layer tambahan dari suatu sistem security

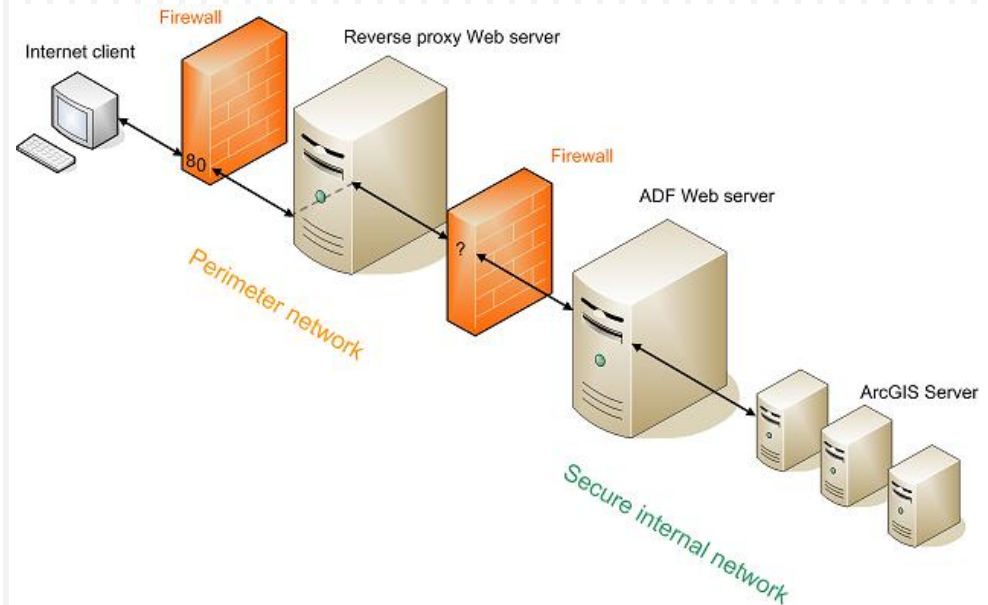
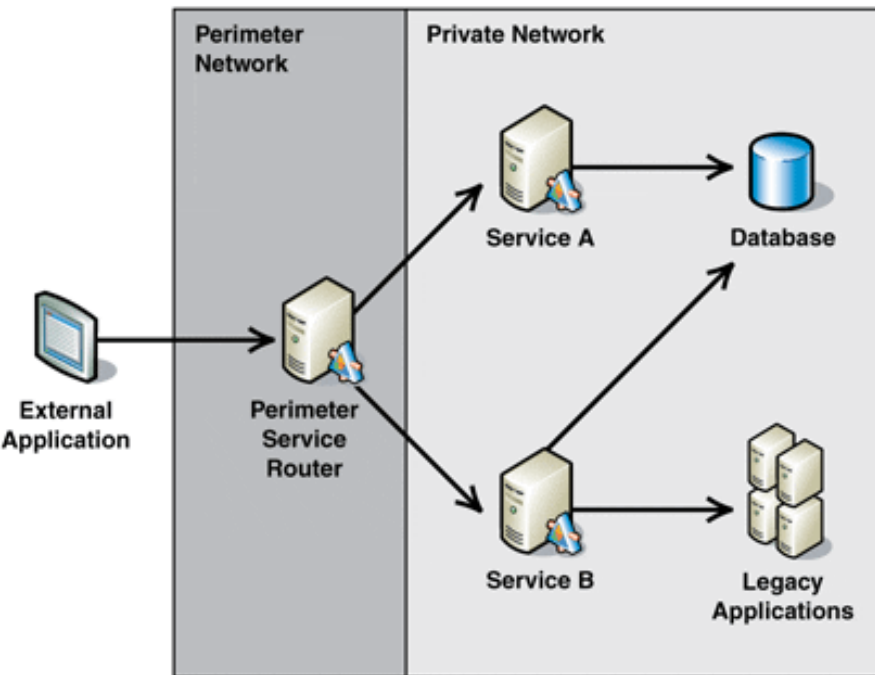
# Peningkatan Keamanan Jaringan

## □ Bastion Host



# Peningkatan Keamanan Jaringan

## □ Perimeter Network



# Peningkatan Keamanan Jaringan

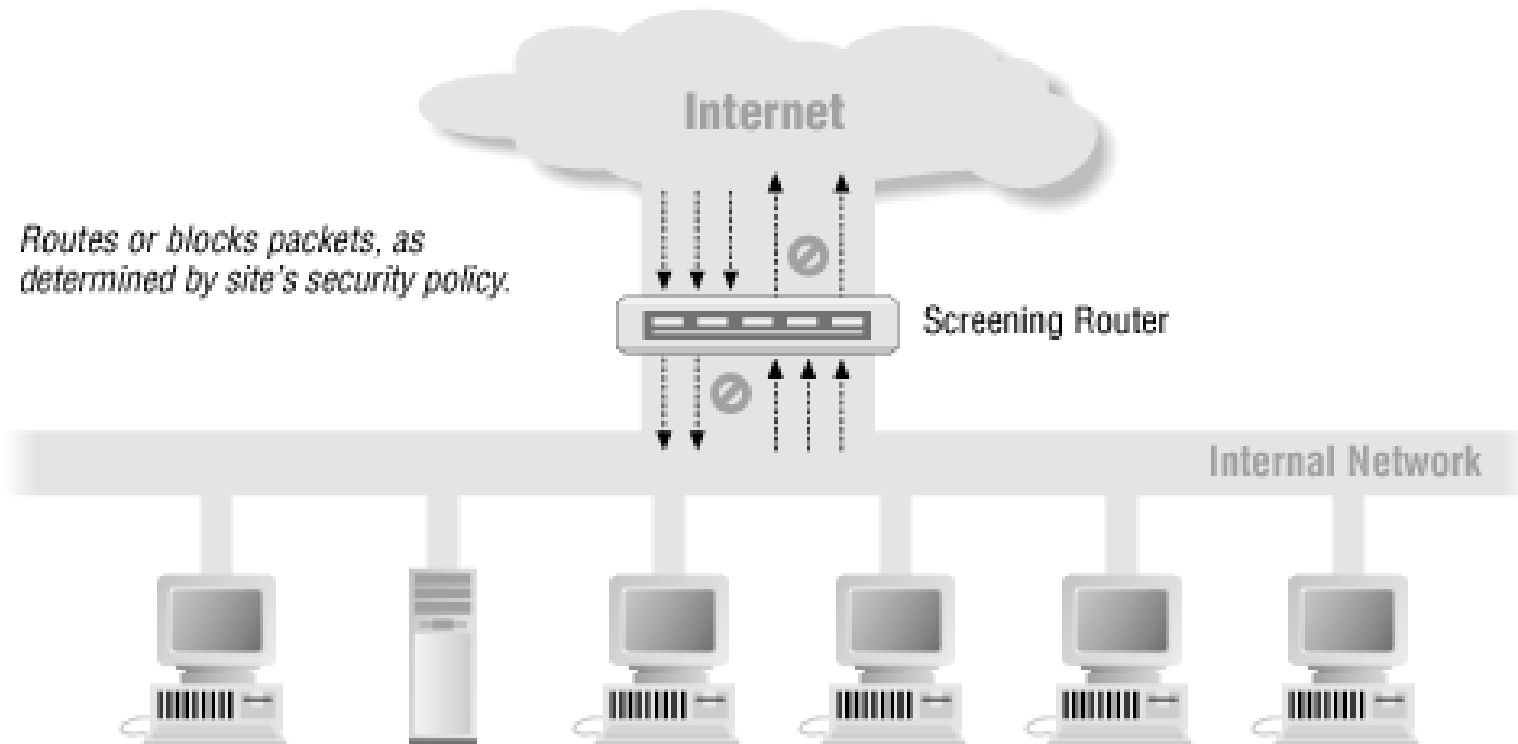
## □ Packet Filtering

- ▣ Sering disebut screening router – router yang melakukan routing packet antara internal dan eksternal network secara selektif sesuai dengan security policy yang digunakan pada network tersebut. Informasi meliputi :

- Ip address asal
- IP address tujuan
- Protocol (TCP, UDP, ICMP)
- Port TCP/UDP asal
- Port TCP/UDP tujuan

# Peningkatan Keamanan Jaringan

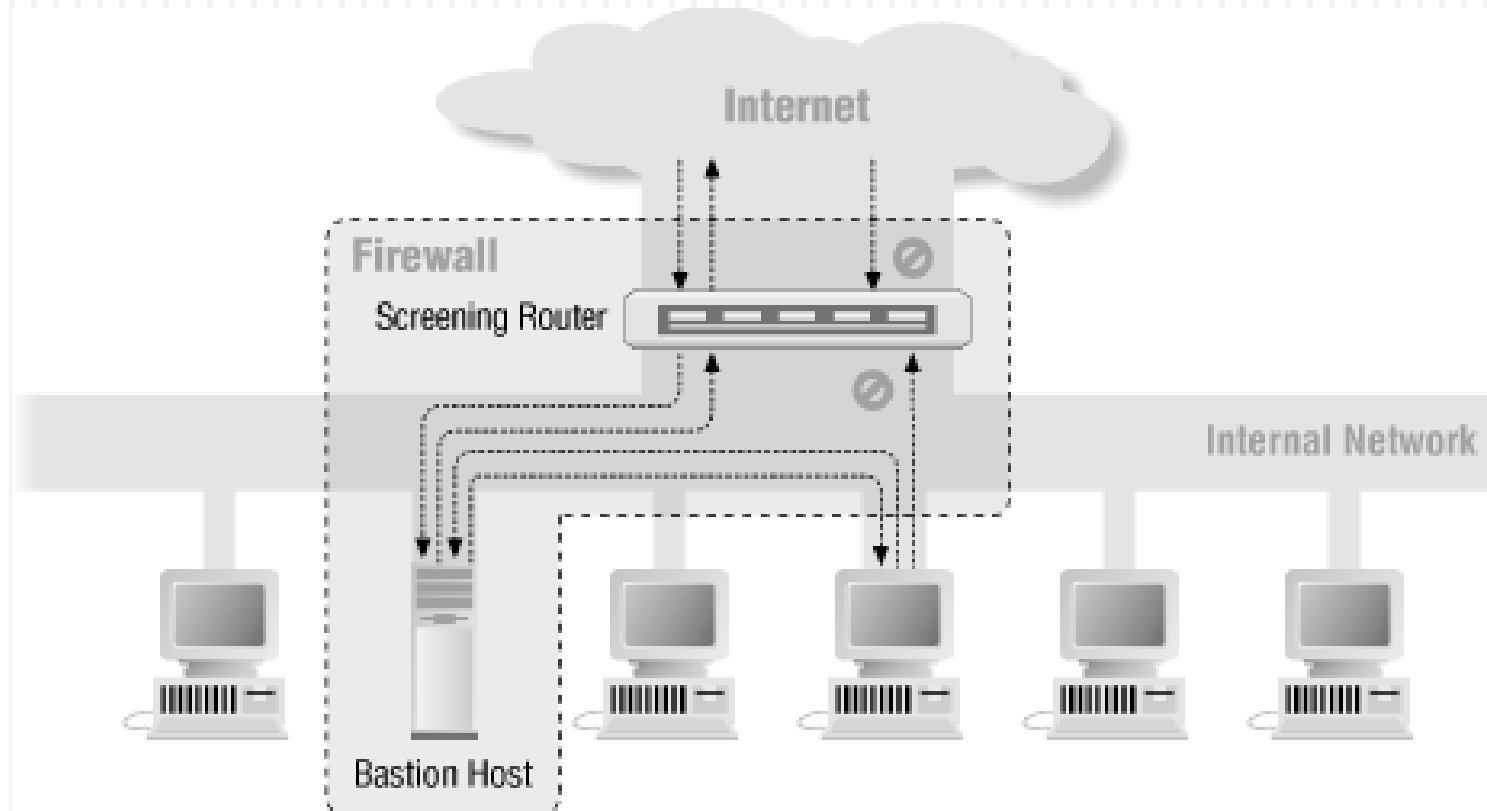
## □ Packet Filtering





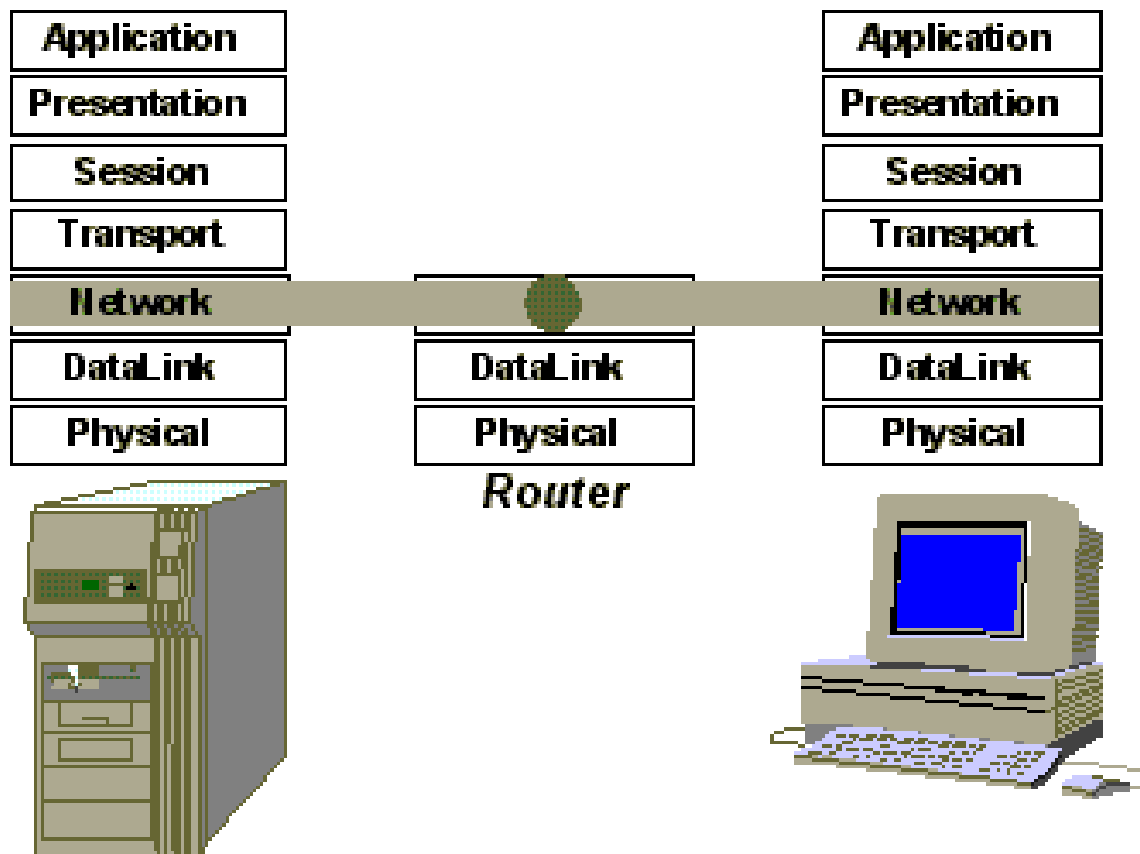
# Peningkatan Keamanan Jaringan

## □ Packet Filtering



# Peningkatan Keamanan Jaringan

## □ Packet Filtering

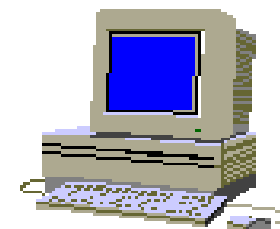
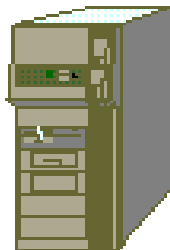


# Peningkatan Keamanan Jaringan

## □ Proxy Services

- ▣ Merupakan aplikasi spesifik atau program server yang dijalankan pada mesin firewall
- ▣ Mengambil request internet service (ftp, telnet, HTTP) dan meneruskan (bergantung pada security policy) ke host yang dituju.
- ▣ Proxy merupakan perantara internal network dan eksternal network (internet)
- ▣ Tingkat sekuritas lebih tinggi dari screening router

## □ Proxy Services



# Peningkatan Keamanan Jaringan

- Variasi Arsitektur Firewall
  - ▣ Kombinasi dari adanya ragam firewall
  - ▣ Konfigurasi disesuaikan dengan kebijakan sekuriti jaringan komputer
    - Dual atau lebih bastion host
    - Menggabungkan ekterior dan interior Router
    - Menggabungkan Bastion Host dan Exterior Router
    - Menggabungkan Bastion Host dan interior router

# Software Firewall

- ❑ Berdasar rule-list yang ada didalamnya
- ❑ Sederhana – GUI
- ❑ Kemampuan

**THANK YOU  
TERIMA KASIH  
HATUR NUHUN  
MATUR SUWUN**



***Mata Kuliah Jaringan Komputer***