Network Security Management

Josua M Sinambela
CompTIA Security+, CCNA

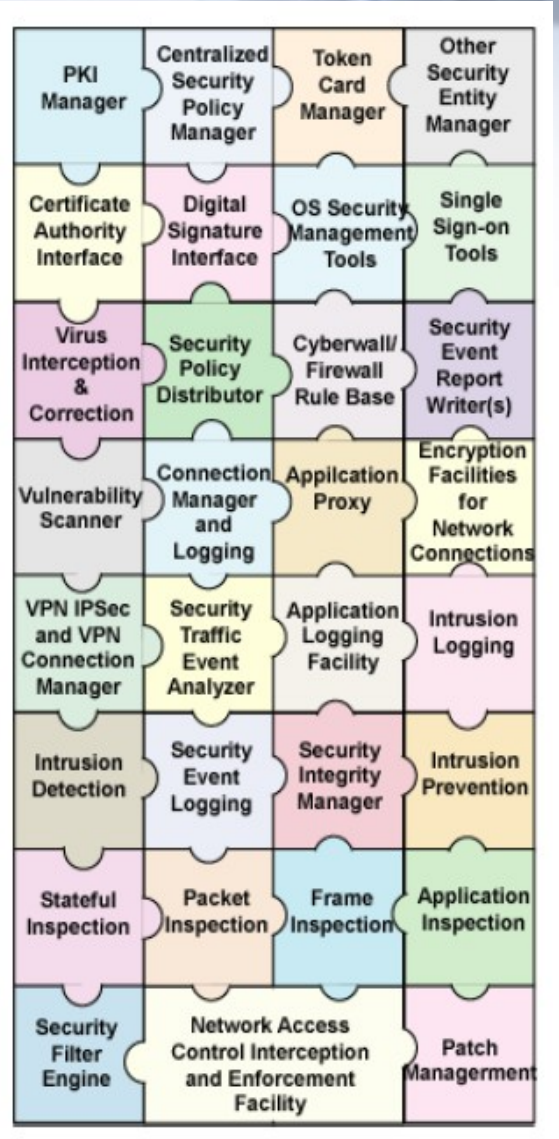
Workshop Metode Pangamanan Jaringan
Pemerintah Kota Yogyakarta
Senin, 3 September 2007
PPTIK UGM, Yogyakarta

Pembahasan

- Prinsip Keamanan
- Disain Jaringan Komputer
- Aplikasi Keamanan Jaringan

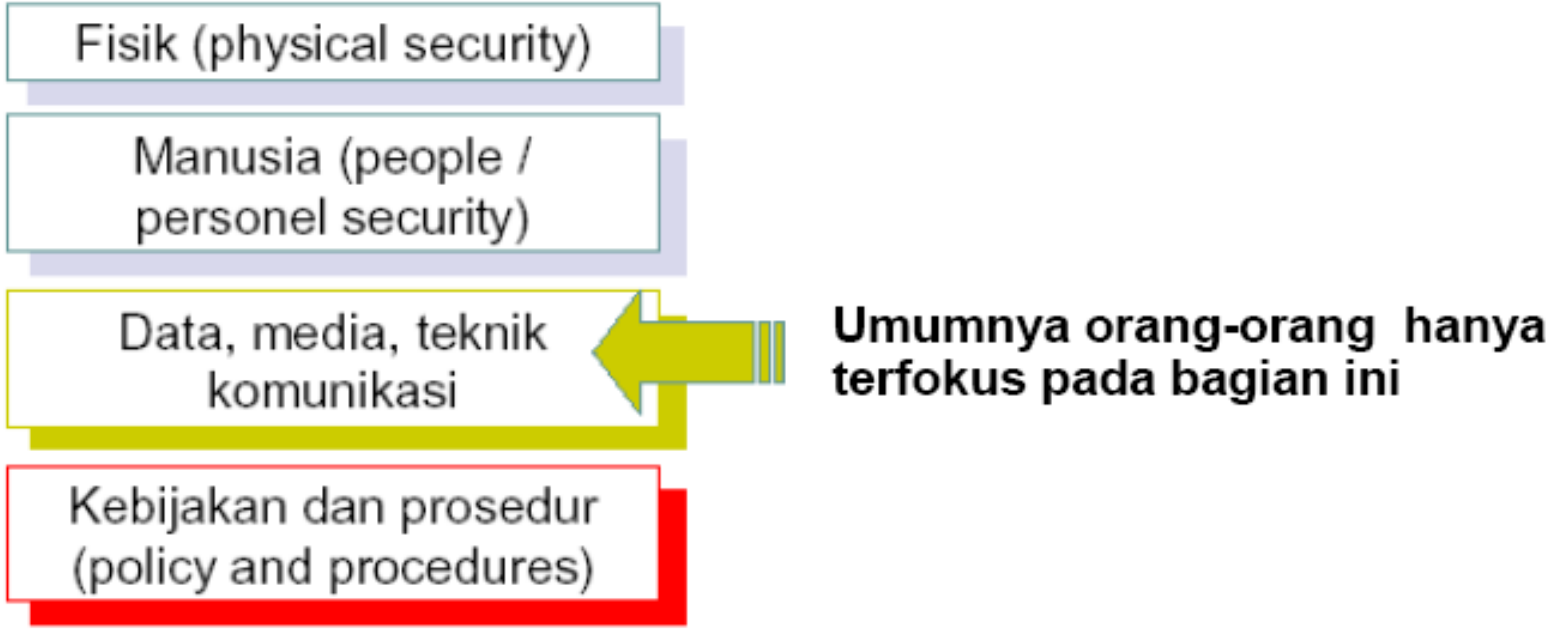
Prinsip Keamanan (intro)

- Keamanan sangat kompleks
  - Terdiri dari banyak bagian atau komponen
  - Tiap komponen masih kompleks
  - Terdapat sangat banyak keahlian khusus dibidang keamanan
  - Tersedia sangat banyak standart
  - Jumlah dan jenis serangan terhadap keamanan bertambah sangat cepat



Prinsip Keamanan (intro)

- Klasifikasi Keamanan menurut David Icove



Prinsip Keamanan (intro)

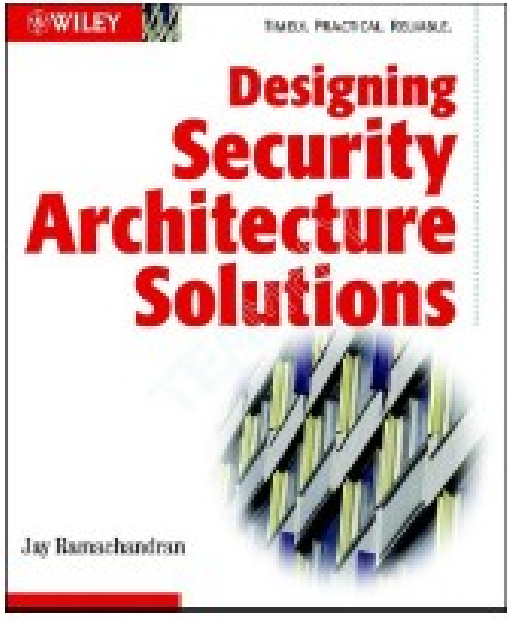
Berdasarkan Elemen System :

- Network security
  - difokuskan pada saluran (media) pembawa informasi atau jalur yang dilalui.
- Application security
  - difokuskan pada aplikasinya sistem tersebut, termasuk database dan servicesnya.
- Computer security
  - difokuskan pada keamanan dari komputer pengguna (end system) yang digunakan untuk mengakses aplikasi, termasuk operating system (OS)

Prinsip Keamanan

Menurut Jay Ramachandran pada bukunya "Designing Security Architecture Solutions"

- Authentication
- Authorization atau Access Control
- Privacy / confidentiality
- Integrity
- Availability
- Non-repudiation
- Auditing



Authentication

- Menyatakan bahwa data atau informasi yang digunakan atau diberikan oleh pengguna adalah benar-benar asli milik pengguna tersebut, demikian juga dengan server dan sistem informasi yang diakses, merupakan server atau sistem informasi yang dituju (Idealnya terjadi mutual otentikasi)
- Serangan pada jaringan berupa DNS Corruption atau DNS Poison, terminal palsu (spooffing), situs aspal dan palsu, user dan password palsu.
- Countermeasure: Digital Signature atau Digital Certificate misalnya teknologi SSL/TLS untuk web dan mail server.

Authorization atau Access Control

- Pengaturan siapa dapat melakukan apa, atau akses dari mana menuju ke mana.
- Dapat menggunakan mekanisme user/password atau group/membership.
- Ada pembagian kelas atau tingkatan.
- Implementasi : pada “ACL” antar jaringan, pada “ACL” proxy server (mis. pembatasan bandwidth/delaypools).

Privacy/confidentiality

- Keamanan terhadap data data pribadi, messages/pesan-pesan atau informasi lainnya yang sensitif.
- Serangan pada jaringan berupa aktifitas sniffing (penyadapan) dan adanya keylogger. Umumnya terjadi karena kebijakan/policy yang kurang jelas.
- Siapa yang paling mungkin melakukan ? Admin atau ISP nakal ?
- Countermeasure : gunakan teknologi enkripsi/kriptografi.

Integrity

- Bahwa informasi atau pesan dipastikan tidak dirubah atau berubah.
- Serangan pada jaringan dapat berupa aktifitas spoofing, mail modification, trojan horse, MITM attack.
- Countermeasure : dengan teknologi digital signature dan Kriptografi spt PGP, 802.1x, WEP, WPA

Availability

- Keamanan atas ketersediaan layanan informasi dan infrastruktur.
- Serangan pada jaringan: DoS (denial of services) baik disadari/sengaja maupun tidak. Aktifitas malware, worm, virus dan bomb mail sering memacetkan jaringan.
- Countermeasure : Firewall dan router filtering, backup dan redundancy, IDS dan IPS

Non-repudiation

- Menjaga agar jika sudah melakukan transaksi atau aktifitas online, maka tidak dapat di sangkal.
- Umumnya digunakan untuk aktifitas e-commerce. Misalnya email yang digunakan untuk bertransaksi menggunakan digital signature.
- Pada jaringan dapat menggunakan digital signature, sertifikat dan kriptografi.
- Contoh kasus, mail.jogja.go.id ? Mail Spoofing masih di mungkinkan terjadi? Check mail open relay

Auditing

- Adanya berkas semacam rekaman komunikasi data yang terjadi pada jaringan untuk keperluan audit seperti mengidentifikasi serangan-serangan pada jaringan atau server.
- Penting memperhatikan space HDD untuk file logging (management log)
- Contoh Implementasi : pada firewall (IDS/IPS) atau router menggunakan system logging (syslog)

Contoh logging sederhana

[root@spider cisco]# **tail -f /var/log/cisco/log.cisco**

Feb 28 14:48:51 cat3550 111063: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.113(1027) -> 172.20.2.3(53), 14 packets

Feb 28 14:48:54 cat3550 111064: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted tcp 172.16.19.103(3219) -> 216.200.68.150(21), 1 packet

Feb 28 14:48:58 cat3550 111065: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.80.104(2782) -> 172.20.2.3(53), 1 packet

Feb 28 14:49:07 cat3550 111066: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.114(1036) -> 172.20.2.3(53), 1 packet

Feb 28 14:49:15 cat3550 111067: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.19.158(1025) -> 172.20.2.3(53), 1 packet

Feb 28 14:49:36 cat3550 111068: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.101(1434) -> 172.20.2.3(53), 1 packet

Feb 28 14:49:38 cat3550 111069: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.10.114(1026) -> 172.20.2.3(53), 1 packet

Feb 28 14:49:41 cat3550 111070: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.116(1031) -> 172.20.2.3(53), 3 packets

Feb 28 14:49:42 cat3550 111071: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.13.102(1208) -> 172.20.2.3(53), 1 packet

Feb 28 14:50:10 cat3550 111072: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted tcp 172.16.80.104(2787) -> 209.133.111.198(21), 1 packet

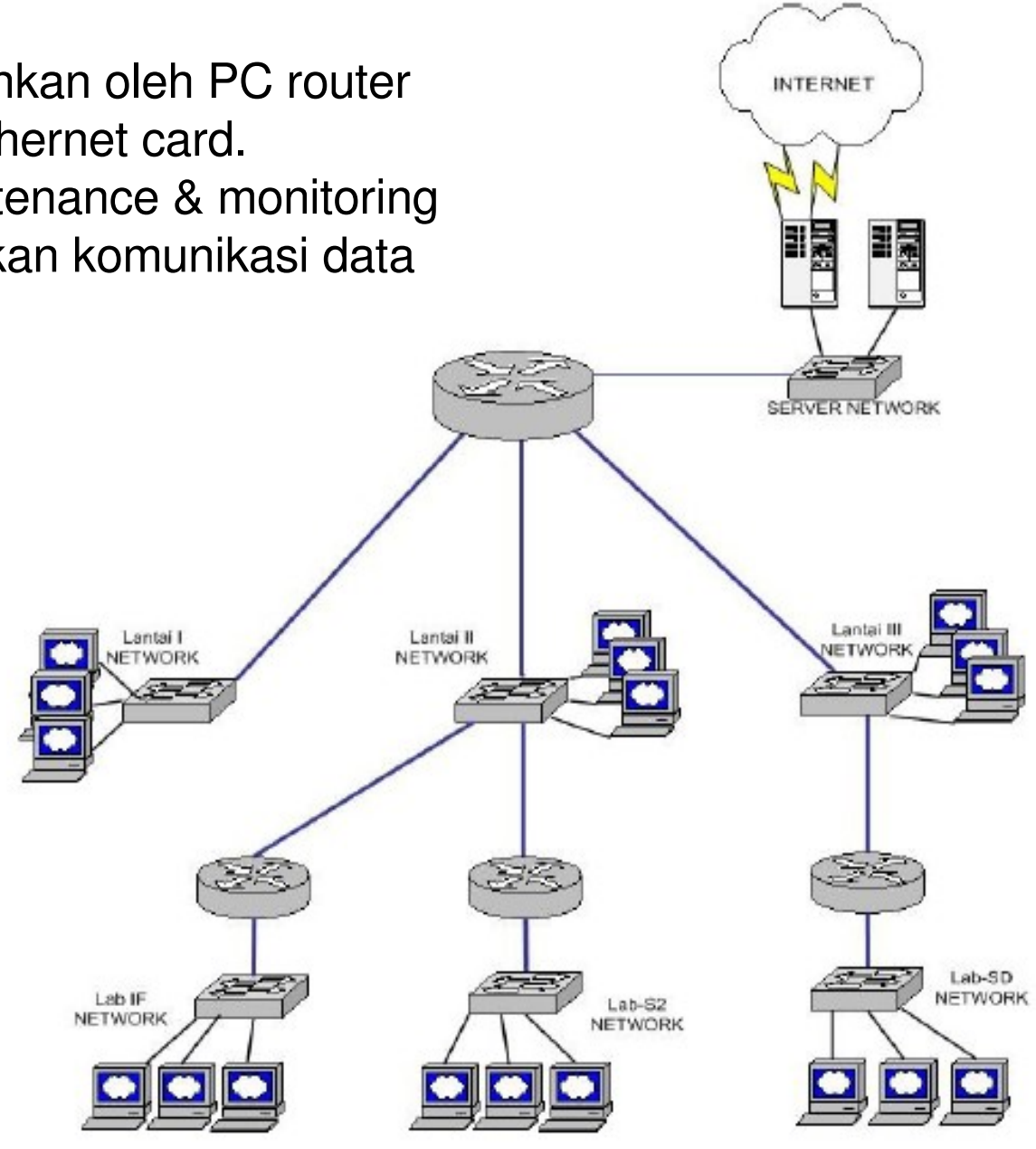
Contoh audit sederhana

```
[root@spider cisco]# perl logscan.pl
Laporan koneksi yang ditolak (denied):
    13:   172.16.10.106  ->    172.16.10.255  udp port 137
     4:   172.16.16.101  ->    172.16.16.255  udp port 137
     3:   172.16.10.106  ->   216.152.244.84  tcp port 80
     2:   172.16.10.106  ->   221.142.186.37  tcp port 445
     2:   172.16.16.115  ->    216.49.88.118  tcp port 80
     1:   172.16.19.158  ->     213.61.6.18  tcp port 50131
     1:   172.16.16.114  ->    120.40.59.62  tcp port 445
     1:   172.16.10.106  ->    172.16.171.5  tcp port 445
     1:   172.16.16.101  ->   87.216.223.241  tcp port 445
     1:   172.16.16.113  ->   61.101.124.133  tcp port 445
     1:   172.16.10.106  ->  149.162.106.255  tcp port 445
     1:   172.16.10.106  ->   185.38.118.127  tcp port 445
     1:   172.16.16.101  ->   195.193.221.99  tcp port 445
     1:   172.16.16.113  ->  102.160.175.170  tcp port 445
     1:   172.16.16.101  ->   123.123.142.84  tcp port 445
Port port tujuan yang ditolak:
   370: tcp port 445
    18: udp port 137
     8: tcp port 80
     2: udp port 138
     1: tcp port 50131
Alamat IP Asal yang melakukan pelanggaran:
   177: 172.16.10.106
   127: 172.16.16.101
    70: 172.16.16.113
    17: 172.16.16.114
     2: 172.16.16.115
     1: 172.16.19.124
     1: 172.16.19.103
     1: 172.16.19.158
     1: 172.16.19.100
     1: 172.16.24.102
     1: 172.16.80.14
[root@spider cisco]#
```

Disain Jaringan Komputer

Contoh Jaringan TE UGM tahun 2000-2002

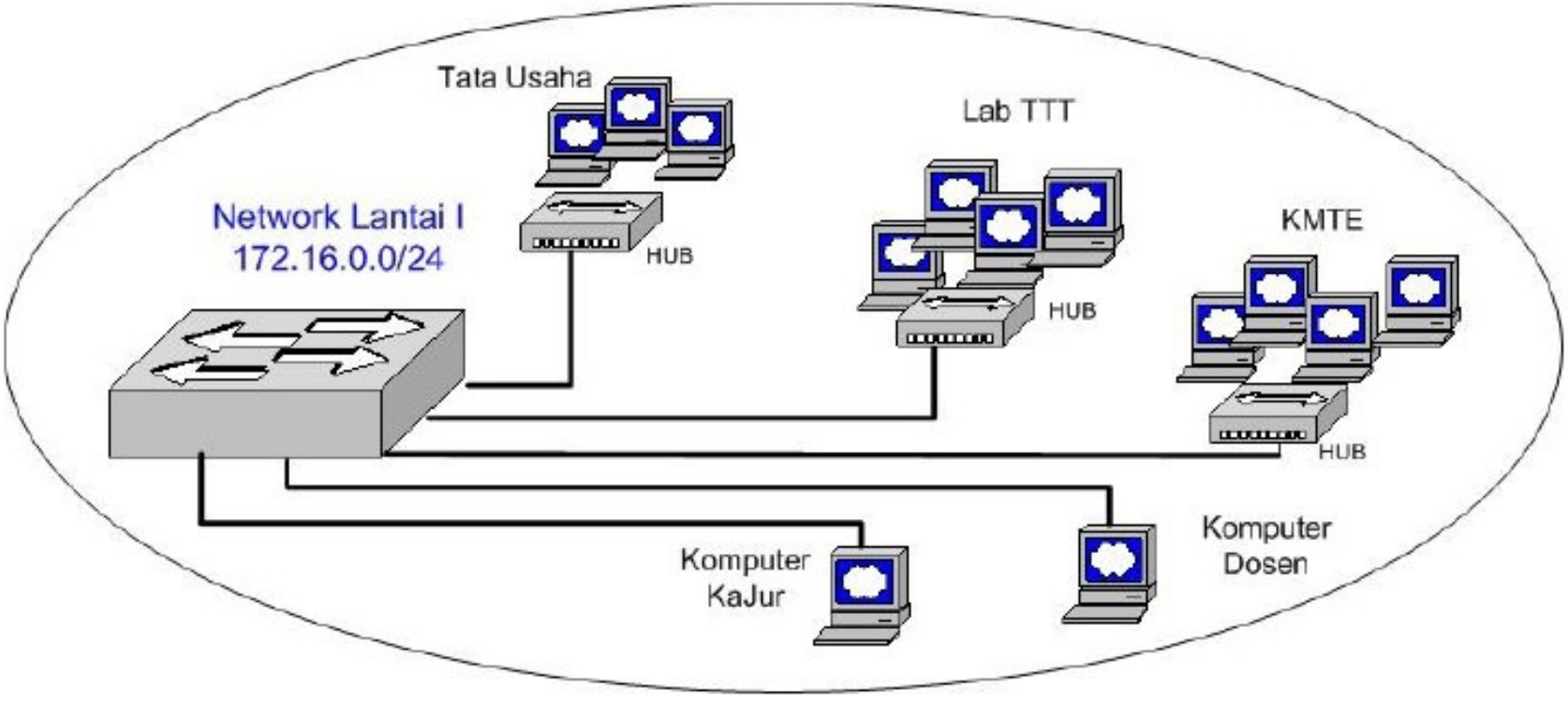
- Jaringan Tradisional
- Setiap network dipisahkan oleh PC router atau butuh sebuah ethernet card.
- Kesulitan dalam maintenance & monitoring
- Kesulitan mengamankan komunikasi data



Disain Jaringan Komputer

Contoh Jaringan TE UGM tahun 2000-2002

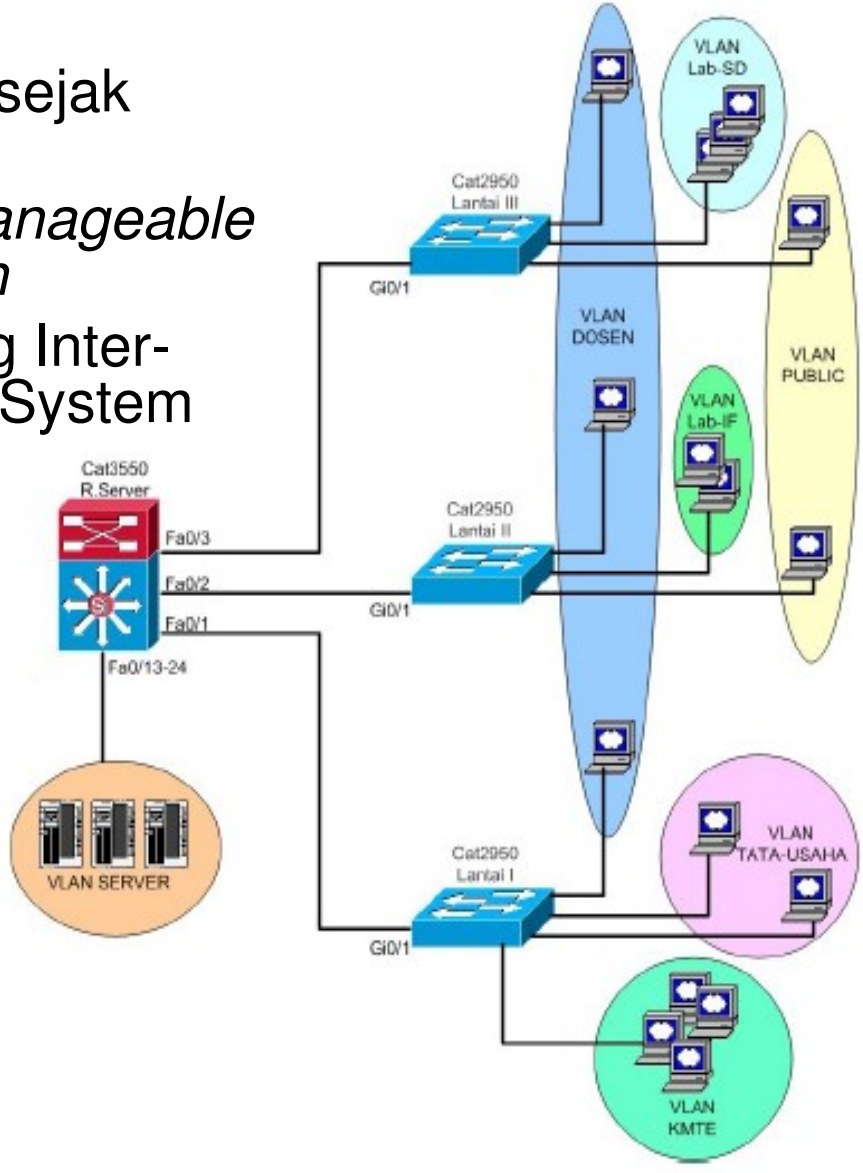
- Lantai I JTE UGM



Disain Jaringan Komputer

Gambaran Jaringan JTE UGM sejak tahun 2003 hingga saat ini

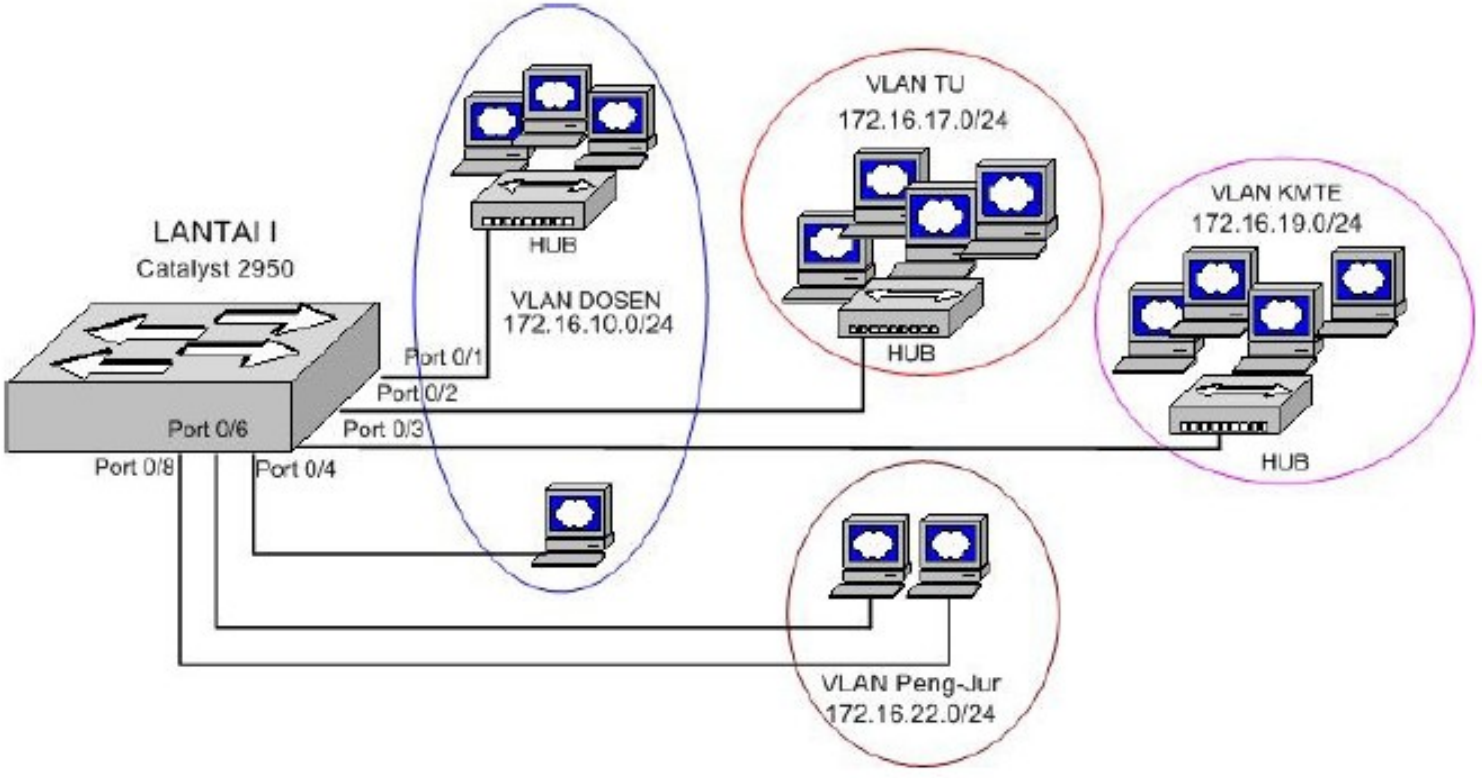
- Menggunakan perangkat *Manageable Switch* dan *Multilayer Switch*
- Implementasi VLAN, Routing Inter-VLAN, Filtering Inter-VLAN, System Logging
- Keuntungan :
  - Skalabilitas
  - Flexibilitas
  - Efisiensi
  - Keamanan Jaringan



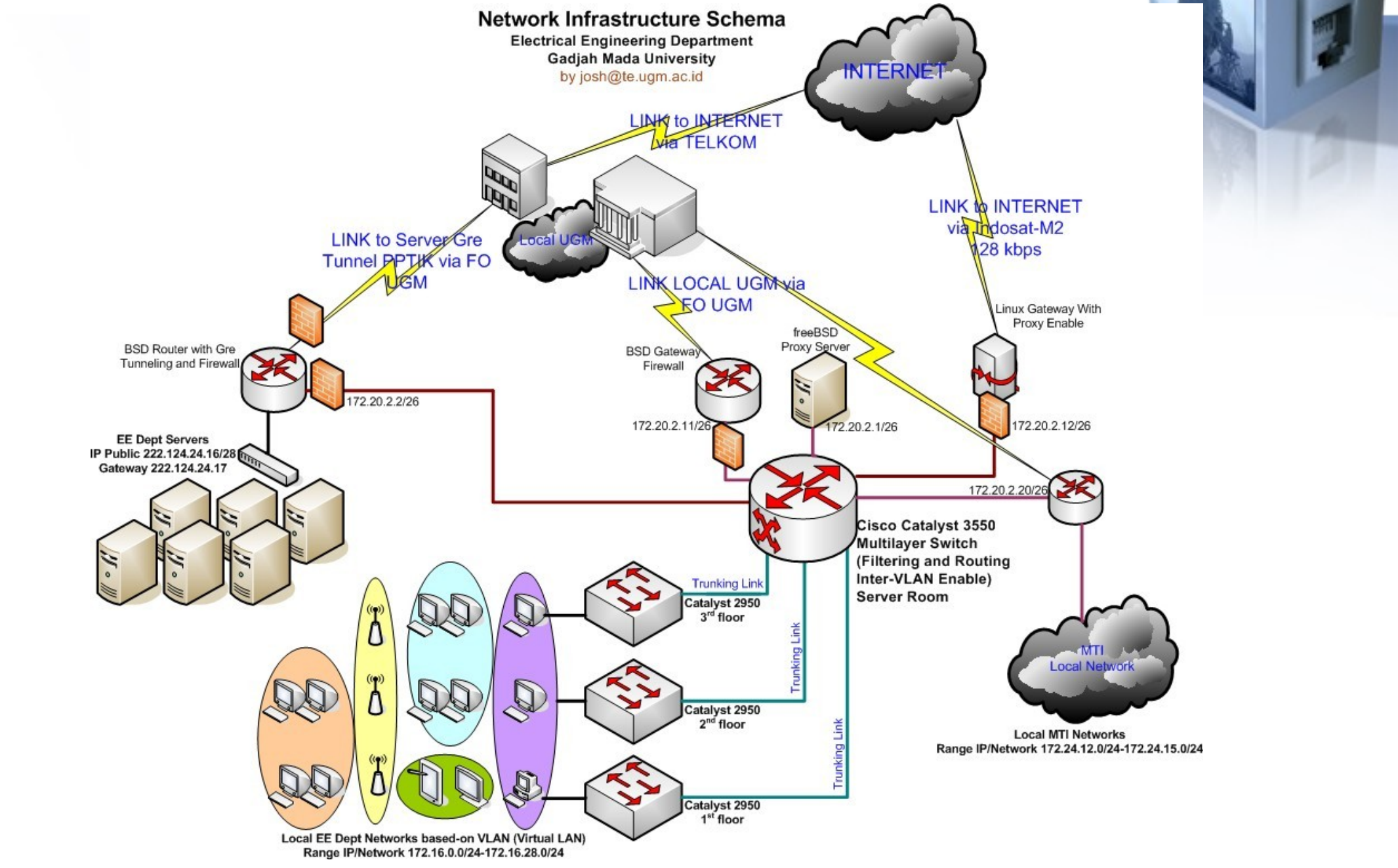
Disain Jaringan Komputer

Contoh Jaringan Lantai I TE UGM sejak 2003-kini

- Lantai I JTE UGM



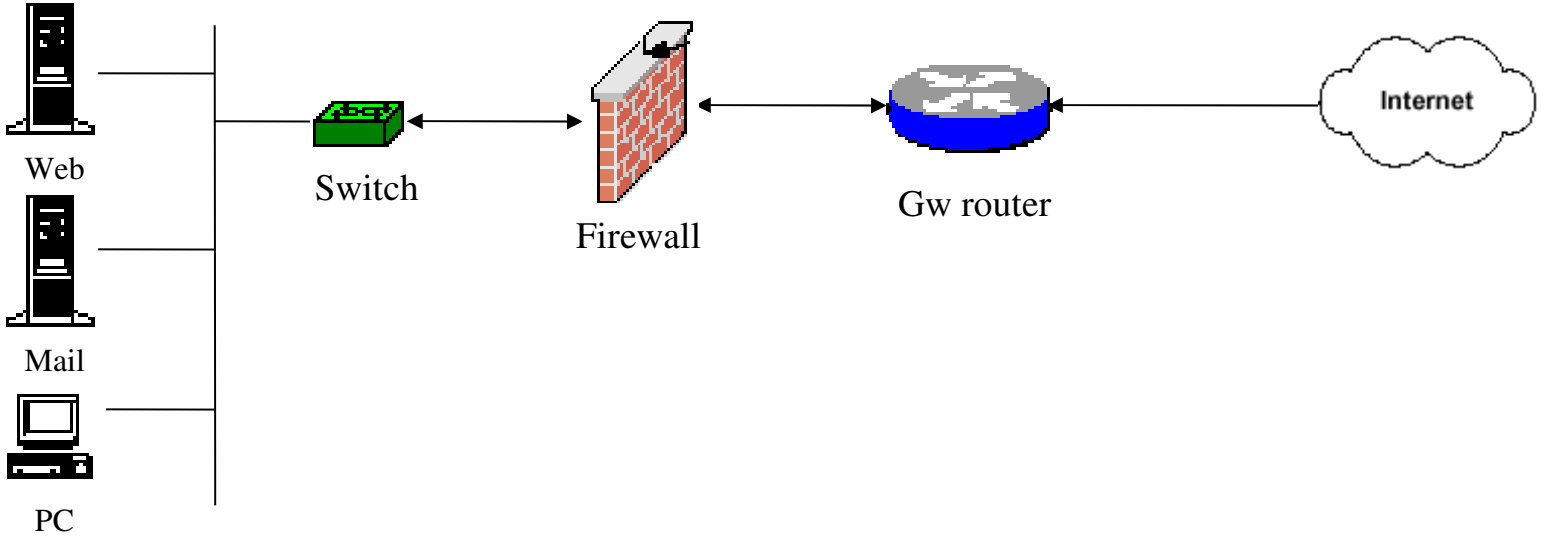
Disain Jaringan Komputer



Aplikasi Keamanan Jaringan

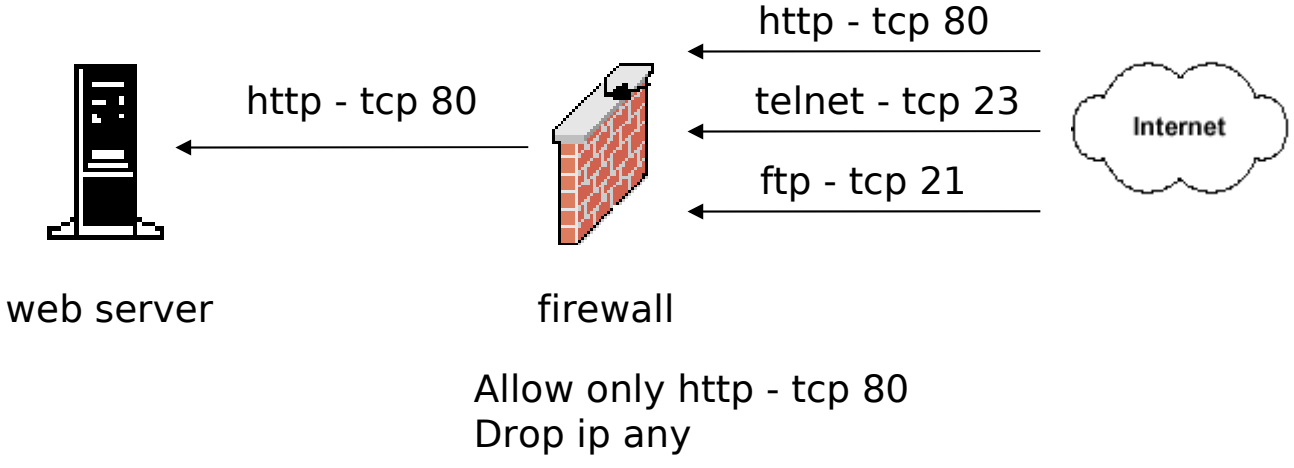
- **Network Firewall**

  Skema umum :



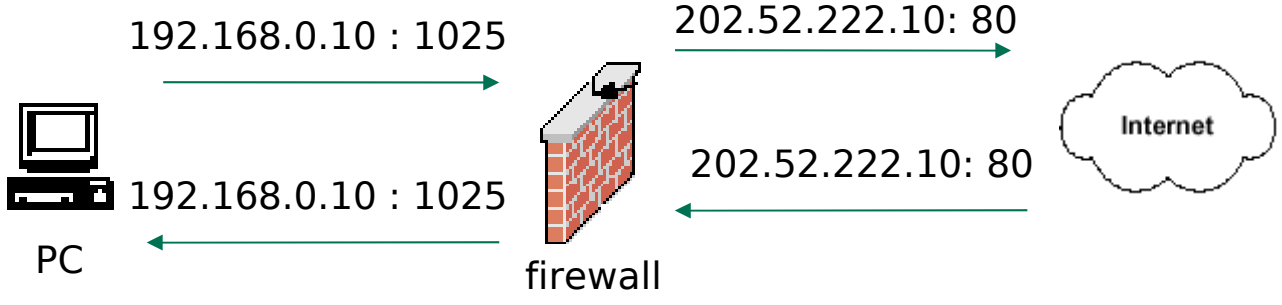
Network Firewall

- **Packet filtering firewalls**
  - **Filtering di layer 3 & 4**



Network Firewall

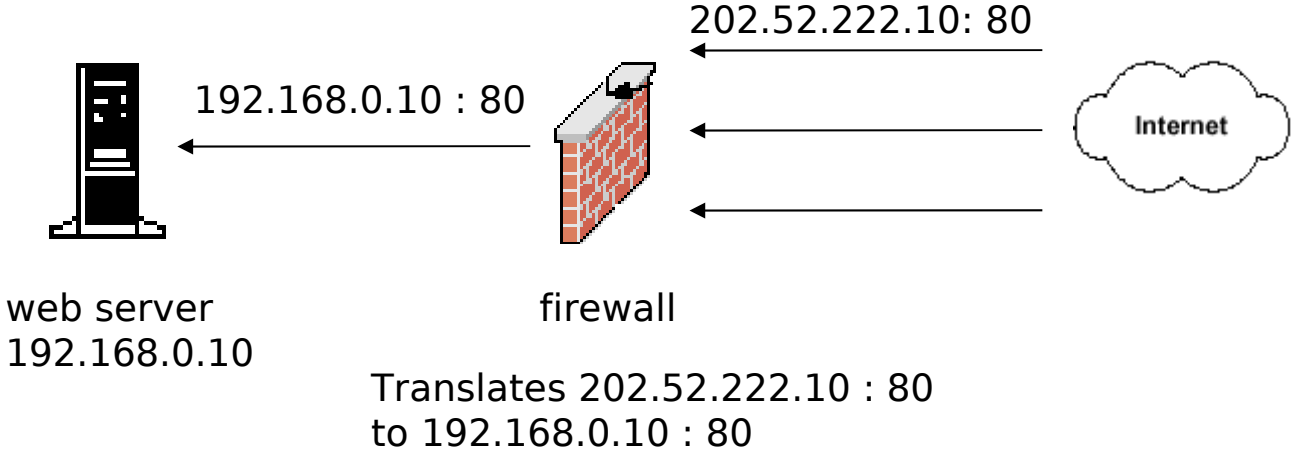
- **Stateful inspection firewalls**
  - **Dipasang pada Gateway**
  - **Memeriksa setiap atribut koneksi yang terjadi untuk setiap client dari awal hingga akhir koneksi**
  - **Cukup Praktis melindungi Jaringan Privat**



Only allows reply packets for
requests made out
Blocks other unregistered traffic

Network Firewall

- **Application layer firewalls**
  - **Filtering di layer Aplikasi**
  - **Disebut juga Proxy Server**



Network Firewall

Product Firewall

– **Iptables**	**www.iptables.org**
– **Ipchains**	**netfilter.samba.org/ipchains**
– **Cisco PIX**	**www.cisco.com**
– **Checkpoint**	**www.checkpoint.com**
– **Border Manager**	**www.novell.com**
– **Winroute**	**www.winroute.com**
– **SonicWall**	**www.sonicwall.com**
– **Juniper**	**www.juniper.net**

Aplikasi Keamanan Jaringan

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

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

Intrusion Detection System

- Jenis IDS
  - Network-based (NIDS)
    memantau anomali di level jaringan,
    misal melihat adanya network scanning
  - Host-based (HIDS)
    memantau anomali di host,
    misal memonitor logfile, process, file ownership,file permission

Intrusion Detection System

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

Q&A ?

TERIMA KASIH