# Mengamankan Sistem Informasi

Gentisya Tri Mardiani, S.Kom

# Bentuk Pengamanan

- Preventif

  contoh:

- Recovery

  contoh:

# Cara Pengamanan

- Mengatur akses (access control)
- Menutup service yang tidak digunakan
- Memasang proteksi
- Firewall
- Pemantau serangan
- Pemantau integritas sistem
- Audit: mengamati berkas log
- Backup secara rutin

# Access Control

- Password

- Kombinasi beberapa karakter
- Apabila valid, pemakai diperbolehkan menggunakan sistem. Apabila ada yang salah, pemakai tidak dapat menggunakan sistem. Informasi tentang kesalahan ini biasanya dicatat dalam berkas *log.*

# Access Control

- Password

- **Serangan:**

  Program "*password cracker*" : tidak dapat mencari tahu kata kunci dari kata yang sudah terenkripsi, tetapi yang dilakukan oleh program ini adalah melakukan coba-coba (*brute force attack*).
- Salah satu caranya adalah mengambil kata dari kamus (*dictionary)* kemudian mengenkripsinya.
- memiliki beberapa algoritma *heuristic* seperti menambahkan angka di belakangnya, atau membaca dari belakang (terbalik),

# Access Control

- Memilih Password, hal yang tidak boleh:

- Nama anda, nama keluarga, ataupun nama kawan.
- Nama komputer yang anda gunakan.
- Nomor telepon atau plat nomor kendaran anda.
- Tanggal lahir.
- Alamat rumah, nama tempat yang terkenal.
- Kata-kata yang terdapat dalam kamus (bahasa Indonesia maupun bahasa Inggris).
- Password dengan karakter yang sama diulang-ulang.
- Hal-hal di atas ditambah satu angka.

# Menutup service yang tidak digunakan

- Kurangnya pengetahuan tentang servis-servis yang memang telah aktif secara *default* setelah menginstal sistem komputer → menjadi celah atau lubang keamanan.
- Cara menutup service:
  - **klik Start → Control Panel → Administrative tools →Services.**
  - Jika statusnya adalah **started** berarti port sedang terbuka
  - **kanan di salah satu service → properties → ubah startup type menjadi disable.**

# Memasang Proteksi

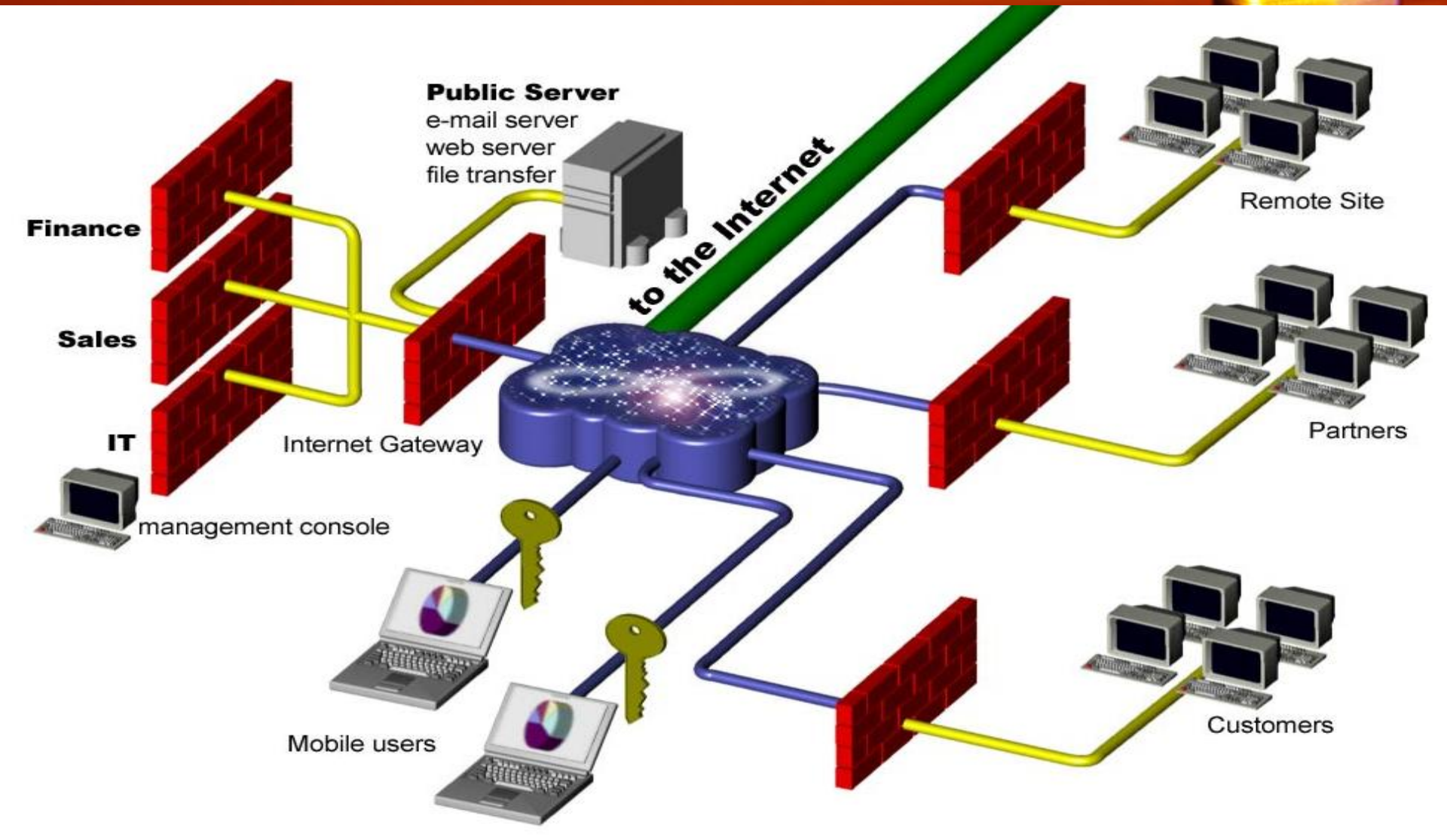
- Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik adalah firewall.

- Filter dapat digunakan untuk memfilter e-mail, informasi, akses, atau bahkan dalam *level package* tertentu. Penangkal lainnya adalah untuk memproteksi sistem kita adalah dengan memasang, meng-update terus anti virus.

# Firewall

- Sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya.

# Firewall


Public Server
e-mail server
web server
file transfer
to the Internet
Finance
Sales
IT
Internet Gateway
management console
Remote Site
Partners
Customers
Mobile users

# Firewall

- Tujuan utama dari 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 pada kebijaksanaan (*policy*) dari organisasi seperti:
  - Hal-hal yang dilarang (*prohibitted*)
  - Hal-hal yang diperbolehkan (*permitted*)

# 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 yang dikonfigurasi menjadi firewall.

# Fungsi Firewall

1. **Mengontrol dan mengawasi paket data yang mengalir di jaringan**. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.

   Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain:

   - Alamat IP dari komputer sumber.
   - Port TCP/UDP sumber dari sumber.
   - Alamat IP dari komputer tujuan.
   - Port TCP/UDP tujuan data pada komputer tujuan
   - Informasi dari header yang disimpan dalam paket data.

# Fungsi Firewall

2. **Melakukan autentifikasi terhadap akses.**

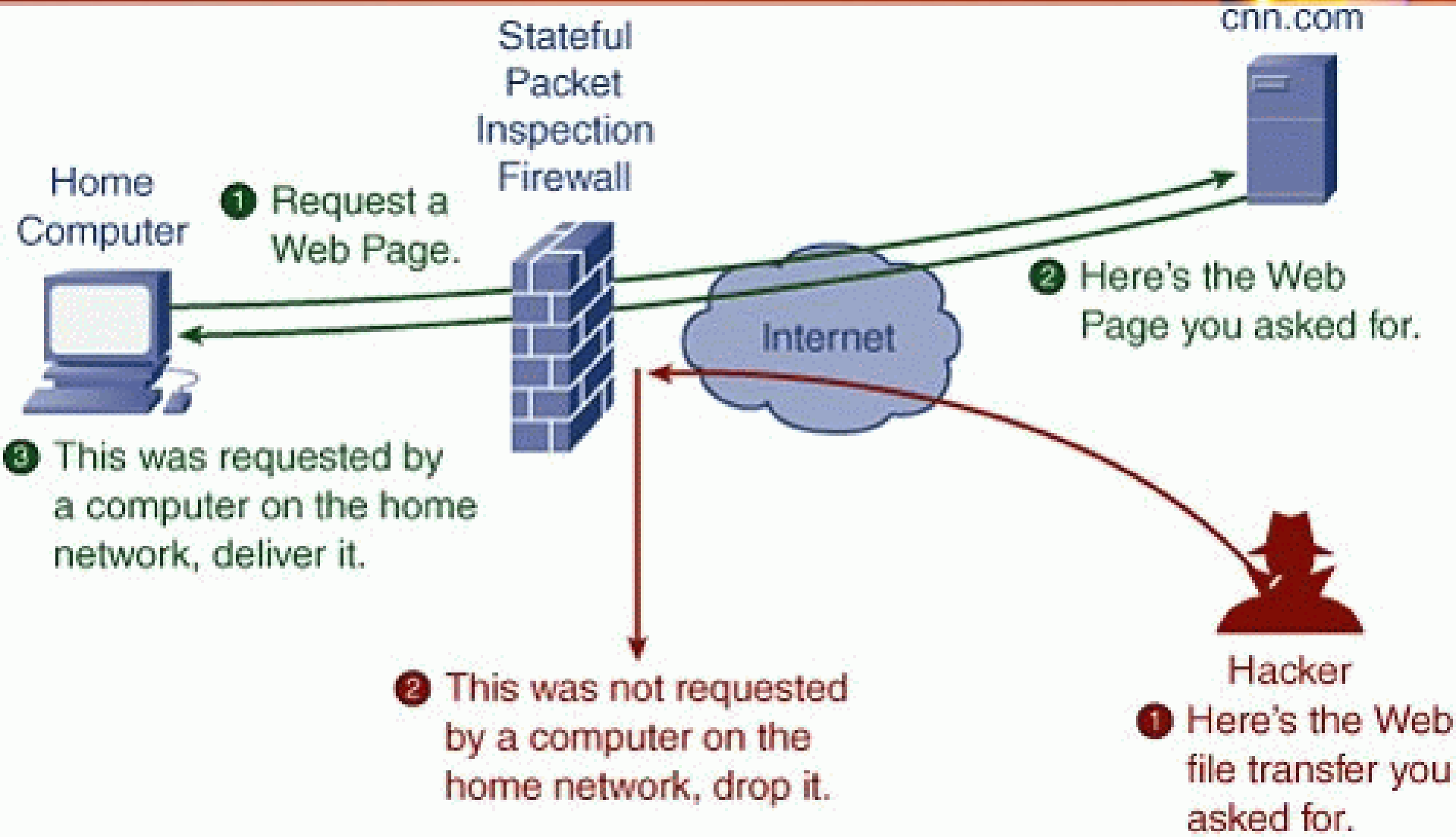
3. **Aplikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data.** Kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. **Mencatat setiap transaksi kejadian yang terjadi di firewall**. Hal ini memungkinkan membantu sebagai pendeteksian dini akan penjebolan jaringan.

# Stateful Packet Inspection Firewall

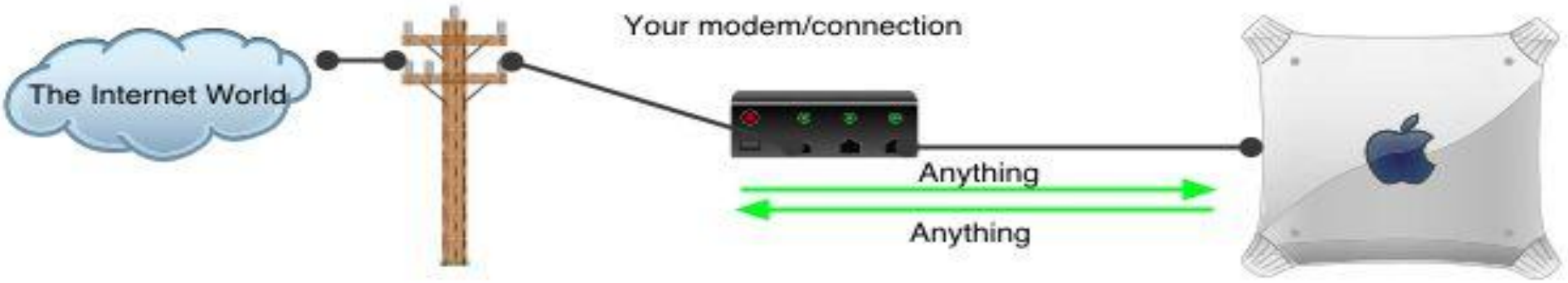
- SPI merupakan proses inspeksi paket data yang mengizinkan firewall untuk melakukan penapisan tidak hanya berdasarkan isi paket tersebut, tapi juga berdasarkan koneksi atau keadaan koneksi, sehingga dapat mengakibatkan firewall memiliki kemampuan yang lebih fleksibel, mudah diatur, dan memiliki skalabilitas dalam hal penapisan yang tinggi.

# Stateful Packet Inspection Firewall

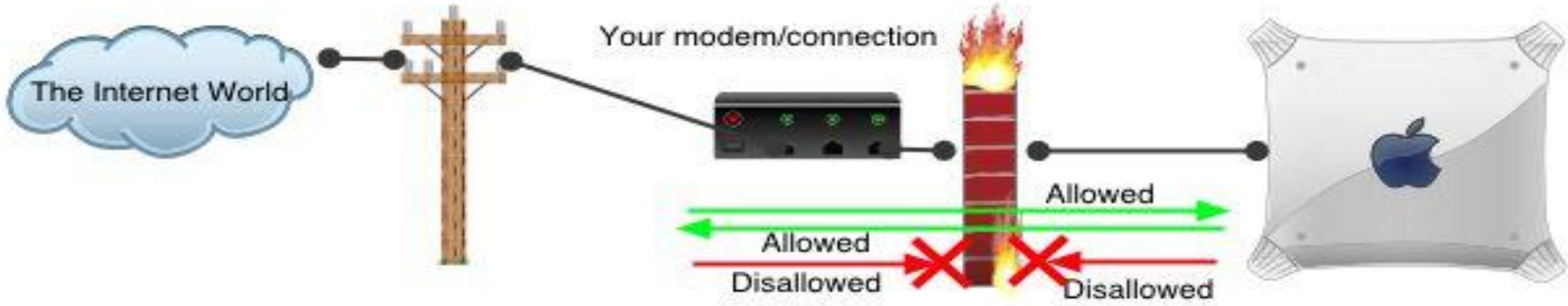


# Firewall

## Without a firewall




## With a firewall



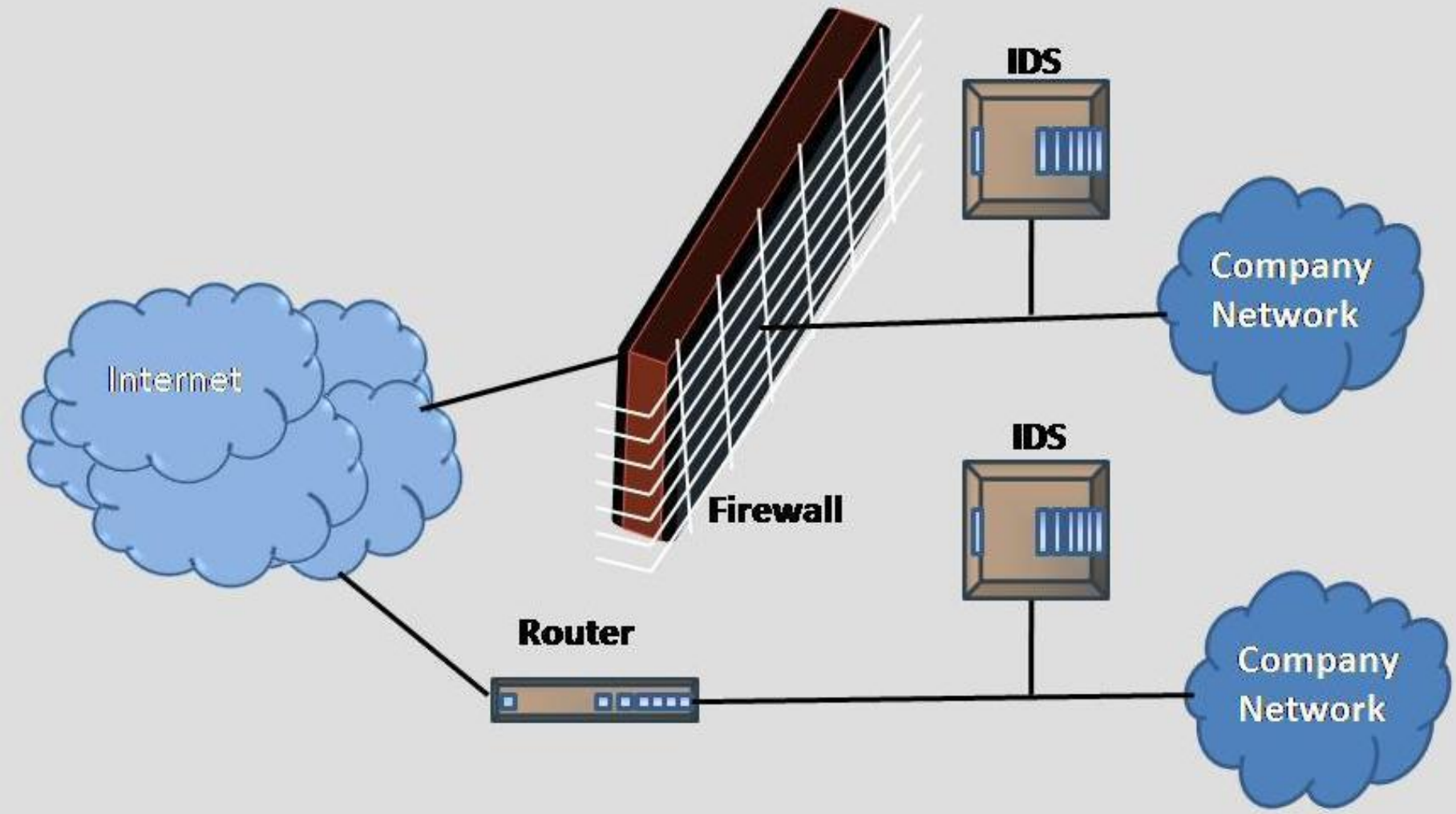
# Pemantau Serangan

- Sistem pemantau (*monitoring system)* digunakan untuk mengetahui adanya tamu tak diundang (*intruder*) atau adanya serangan (*attack*).
- Nama lain dari sistem ini adalah *Intrusion Detection System* (IDS).
- Sistem ini dapat memberitahu administrator melalui e-mail maupun melalui mekanisme lain seperti melalui pager.

# Pemantau Serangan

- *Intrusion Detection System* (IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.
- IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

# IDS


IDS
Company Network
Internet
IDS
Firewall
Router
Company Network

# Jenis IDS

- *Network-based Intrusion Detection System* (NIDS): Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan.

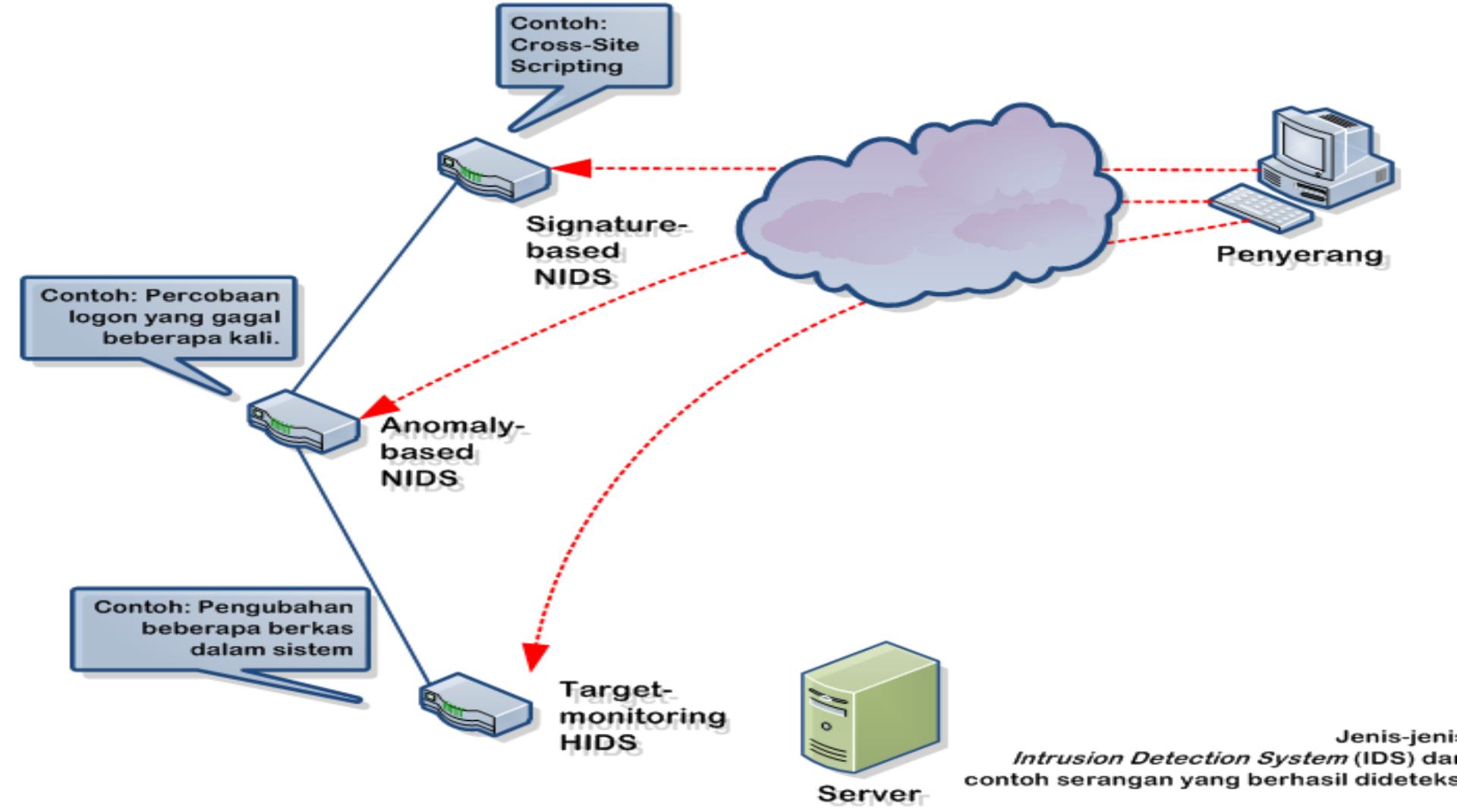
  NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan *switch* Ethernet.

# Jenis IDS

- *Host-based Intrusion Detection System* (HIDS): Aktivitas sebuah *host* jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak.

  HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya *firewall*, *web server*, atau server yang terkoneksi ke Internet.

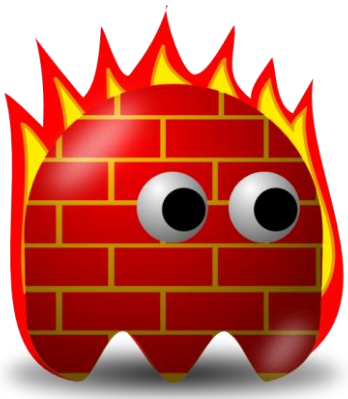
# Jenis IDS




Jenis-jeni
*Intrusion Detection System* (IDS) da
contoh serangan yang berhasil dideteks

# Produk IDS

- RealSecure dari Internet Security Systems (ISS).
- Cisco Secure Intrusion Detection System dari Cisco Systems.
- eTrust Intrusion Detection dari Computer Associates.
- Symantec Client Security dari Symantec
- Computer Misuse Detection System dari ODS Networks
- Kane Security Monitor dari Security Dynamics
- Cybersafe , Network Associates , Network Flight Recorder , Intellitactics , SecureWorks
- Snort (open source)



See you next week...