HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

CƠ SỞ AN TOÀN THÔNG TIN

NỘI DUNG 5 – CÁC KỸ THUẬT VÀ CÔNG CỤ ĐẢM BẢO ATTT

Giảng viên: TS. Đinh Trường Duy

Điện thoại/E-mail: duydt@ptit.edu.vn

Khoa: An toàn thông tin

Nội dung bài giảng dựa trên bài giảng và giáo trình An toàn và bảo mật hệ thống thông tin của TS. Hoàng Xuân Dậu

NỘI DUNG 5

1. Điều khiển truy nhập
2. Tường lửa
3. IDS và IPS

5.1 Điều khiển truy nhập

1. Khái niệm điều khiển truy nhập
2. Các biện pháp điều khiển truy nhập
3. Một số công nghệ điều khiển truy nhập

5.1.1 Khái niệm điều khiển truy nhập

- Điều khiển truy nhập là quá trình mà trong đó người dùng được *nhận dạng* và *trao quyền* truy nhập đến các thông tin, các hệ thống và tài nguyên.
- Một hệ thống điều khiển truy nhập có thể được cấu thành từ 3 dịch vụ:
  - Xác thực (Authentication):
    - Là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dùng cung cấp.
  - Trao quyền (Authorization):
    - Trao quyền xác định các tài nguyên mà người dùng được phép truy nhập sau khi người dùng đã được xác thực.
  - Quản trị (Administration):
    - Cung cấp khả năng thêm, bớt và sửa đổi các thông tin tài khoản người dùng, cũng như quyền truy nhập của người dùng.

5.1.1 Khái niệm điều khiển truy nhập

- Mục đích chính của điều khiển truy nhập là để đảm bảo tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và các tài nguyên:
  - Tính bí mật (confidentiality): đảm bảo chỉ những người có thẩm quyền mới có khả năng truy nhập vào dữ liệu và hệ thống.
  - Tính toàn vẹn (Integrity): đảm bảo dữ liệu không bị sửa đổi bởi các bên không có đủ thẩm quyền.
  - Tính sẵn dùng: đảm bảo tính sẵn sàng (đáp ứng nhanh/kịp thời) của dịch vụ cung cấp cho người dùng thực sự.

5.1.2 Các biện pháp điều khiển truy nhập

- Điều khiển truy nhập tuỳ chọn – Discretionary Access Control (DAC)
- Điều khiển truy nhập bắt buộc – Mandatory Access Control (MAC)
- Điều khiển truy nhập dựa trên vai trò – Role-Based Access Control (RBAC)
- Điều khiển truy nhập dựa trên luật – Rule-Based Access Control.

5.1.2 Các biện pháp điều khiển truy nhập - DAC

- Điều khiển truy nhập tuỳ chọn được định nghĩa là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên thông tin nhận dạng của các chủ thể và/hoặc nhóm của các chủ thể.
- Thông tin nhận dạng có thể gồm:
  - Bạn là ai? (CMND, bằng lái xe, vân tay,...)
  - Những cái bạn biết (tên truy nhập, mật khẩu, số PIN...)
  - Bạn có gì? (Thẻ ATM, thẻ tín dụng, ...)

5.1.2 Các biện pháp điều khiển truy nhập - DAC

- DAC cho phép người dùng có thể cấp hoặc huỷ quyền truy nhập cho các người dùng khác đến các đối tượng thuộc quyền điều khiển của họ.
- Chủ sở hữu của các đối tượng (owner of objects) là người dùng có toàn quyền điều khiển các đối tượng này.

5.1.2 Các biện pháp điều khiển truy nhập - DAC

- Ví dụ: Với DAC:
  - Người dùng được cấp 1 thư mục riêng và là chủ sở hữu của thư mục này;
  - Người dùng có quyền tạo, sửa đổi và xoá các files trong thư mục của riêng mình (home directory);
  - Họ cũng có khả năng trao hoặc huỷ quyền truy nhập vào các files của mình cho các người dùng khác.

5.1.2 Các biện pháp điều khiển truy nhập – DAC - ACM

- Ma trận điều khiển truy nhập (Access Control Matrix - ACM) là một phương pháp mô tả điều khiển truy nhập thông qua 1 ma trận 2 chiều gồm chủ thể (subject), đối tượng (object) và các quyền truy nhập.
  - Đối tượng/Khách thể (Objects) là các thực thể cần bảo vệ. Objects có thể là các files, các tiến trình (processes).
  - Chủ thể (Subjects) là người dùng (users), tiến trình tác động lên objects.
  - Quyền truy nhập là hành động mà Subject thực hiện trên object.

4.1.2 Các biện pháp điều khiển truy nhập – DAC - ACM

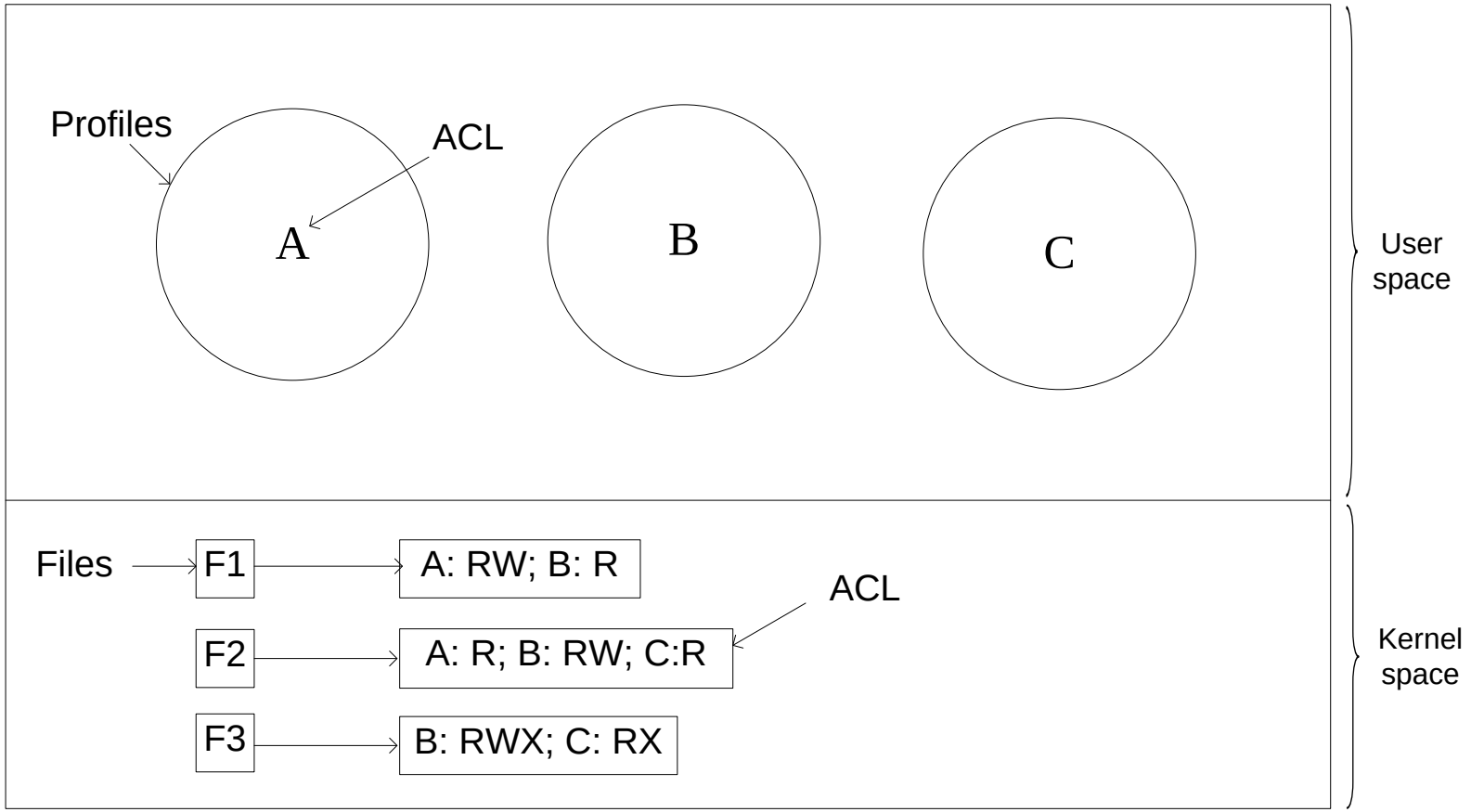
Objects / Subjects	O1	O2	O3	O4
S1	rw	rwxo	r	rwxo
S2	rw	rx	rw	rwx
S3	r	rw	rwo	rw

Các chủ thể: S1, S2, S3
Các đối tượng: O1, O2, O3
Các quyền: r(read), w(write), x(execute) và o(own)

5.1.2 Các biện pháp điều khiển truy nhập – DAC - ACL

- Danh sách điều khiển truy nhập (Access Control List - ACL) là một danh sách các quyền truy nhập của một chủ thể đối với một đối tượng.
  - Một ACL chỉ ra các người dùng hoặc tiến trình được truy nhập vào đối tượng nào và các thao tác cụ thể (quyền) được thực hiện trên đối tượng đó.
  - Một bản ghi điển hình của ACL có dạng (subject, operation). Ví dụ bản ghi (Alice, write) của 1 file có nghĩa là Alice có quyền ghi vào file đó.
  - Khi chủ thể yêu cầu truy nhập, hệ điều hành sẽ kiểm tra ACL xem yêu cầu đó có được phép hay không.
  - ACL có thể được áp dụng cho một hoặc 1 nhóm đối tượng.

5.1.2 Các biện pháp điều khiển truy nhập – DAC - ACL



Sử dụng ACL để quản lý việc truy cập file

5.1.2 Các biện pháp điều khiển truy nhập - MAC

- Điều khiển truy bắt buộc được định nghĩa là các cơ chế hạn chế truy nhập đến các đối tượng dựa trên
  - Tính nhạy cảm (sensitivity) của thông tin (thường được gán nhãn) chứa trong các đối tượng, và
  - Sự trao quyền chính thức (formal authorization) cho các chủ thể truy nhập các thông tin nhạy cảm này.

5.1.2 Các biện pháp điều khiển truy nhập - MAC

❖ Các mức nhạy cảm:

- Tối mật (Top Secret - T): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến những thiệt hại trầm trọng đối với an ninh quốc gia.
- Tuyệt mật (Secret - S): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến một loạt thiệt hại đối với an ninh quốc gia.
- Mật (Confidential - C): Được áp dụng với thông tin mà nếu bị lộ có thể dẫn đến thiệt hại đối với an ninh quốc gia.
- Không phân loại (Unclassified - U): Những thông tin không gây thiệt hại đối với an ninh quốc gia nếu bị tiết lộ.

5.1.2 Các biện pháp điều khiển truy nhập - MAC

- MAC không cho phép người tạo ra các đối tượng (thông tin/tài nguyên) có toàn quyền truy nhập các đối tượng này.
- Quyền truy nhập đến các đối tượng (thông tin/tài nguyên) do người quản trị hệ thống định ra trước trên cơ sở chính sách an toàn thông tin của tổ chức đó.
- MAC thường được sử dụng phổ biến trong các cơ quan an ninh, quân đội và ngân hàng.

5.1.2 Các biện pháp điều khiển truy nhập - MAC

- Ví dụ: một tài liệu được tạo ra và được đóng dấu "Mật":
  - Chỉ những người có trách nhiệm trong tổ chức mới được quyền xem và phổ biến cho người khác;
  - Tác giả của tài liệu không được quyền phổ biến đến người khác.

5.1.2 Các biện pháp điều khiển truy nhập - MAC

❖ Mô hình điều khiển truy nhập Bell-LaPadula:

- Mô hình Bell-La Padula là mô hình bảo mật đa cấp thường được sử dụng trong quân sự, nhưng nó cũng có thể áp dụng cho các lĩnh vực khác.
- Trong quân sự, các tài liệu được gán một mức độ bảo mật, chẳng hạn như không phân loại, mật, bí mật và tối mật. Người dùng cũng được ấn định các cấp độ bảo mật, tùy thuộc vào những tài liệu mà họ được phép xem.
  - Một vị tướng quân đội có thể được phép xem tất cả các tài liệu, trong khi một trung úy có thể bị hạn chế chỉ được xem các tài liệu mật và thấp hơn.
  - Một tiến trình chạy nhân danh một người sử dụng có được mức độ bảo mật của người dùng đó.

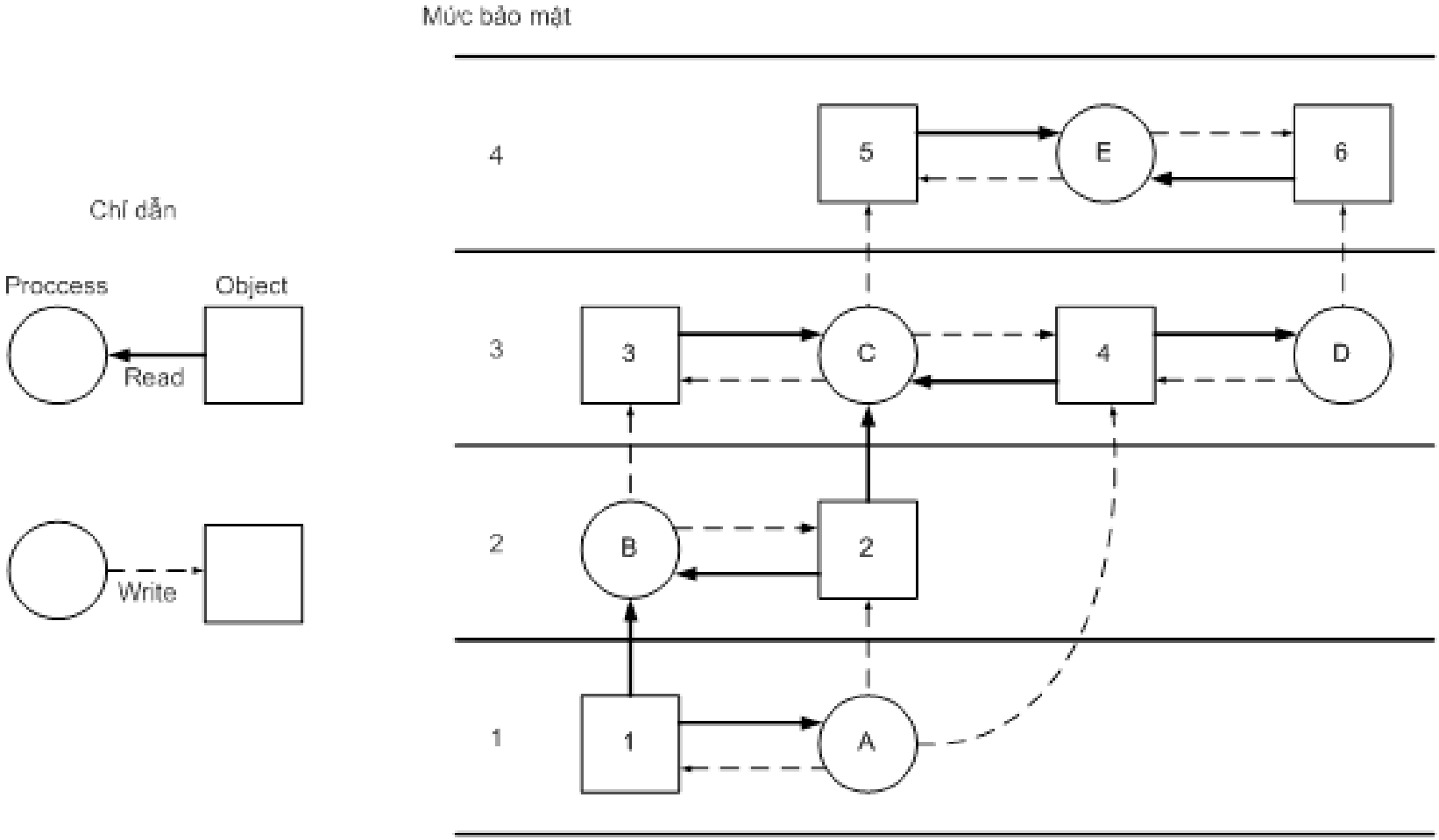
5.1.2 Các biện pháp điều khiển truy nhập - MAC

- Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula:
  - Nguyên tắc đọc xuống:
    - Một người dùng ở mức độ bảo mật k chỉ có thể đọc các đối tượng ở cùng mức bảo mật hoặc thấp hơn.
    - Ví dụ:
      - Một vị tướng có thể đọc các tài liệu của một trung úy;
      - Nhưng một trung úy không thể đọc các tài liệu của vị tướng đó.

5.1.2 Các biện pháp điều khiển truy nhập - MAC

- Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula:
  - Nguyên tắc ghi lên:
    - Một người dùng ở mức độ bảo mật k chỉ có thể ghi các đối tượng ở cùng mức bảo mật hoặc cao hơn.
    - Ví dụ:
      - Một trung úy có thể nối thêm một tin nhắn vào hộp thư của chung về tất cả mọi thứ ông biết;
      - Nhưng một vị tướng không thể ghi thêm một tin nhắn vào hộp thư của trung úy với tất cả mọi thứ ông ấy biết vì vị tướng có thể đã nhìn thấy tài liệu có mức độ bảo mật cao mà không thể được tiết lộ cho một trung úy.

5.1.2 Các biện pháp điều khiển truy nhập - MAC



Mô hình bảo mật đa cấp Bell-LaPadula

5.1.2 Các biện pháp điều khiển truy nhập - RBAC

- Điều khiển truy nhập dựa trên vai trò cho phép người dùng truy nhập vào hệ thống và thông tin dựa trên vai trò (role) của họ trong công ty/tổ chức đó.
- Điều khiển truy nhập dựa trên vai trò có thể được áp dụng cho một nhóm người dùng hoặc từng người dùng riêng lẻ.
- Quyền truy nhập được tập hợp thành các nhóm “vai trò” với các mức quyền truy nhập khác nhau.

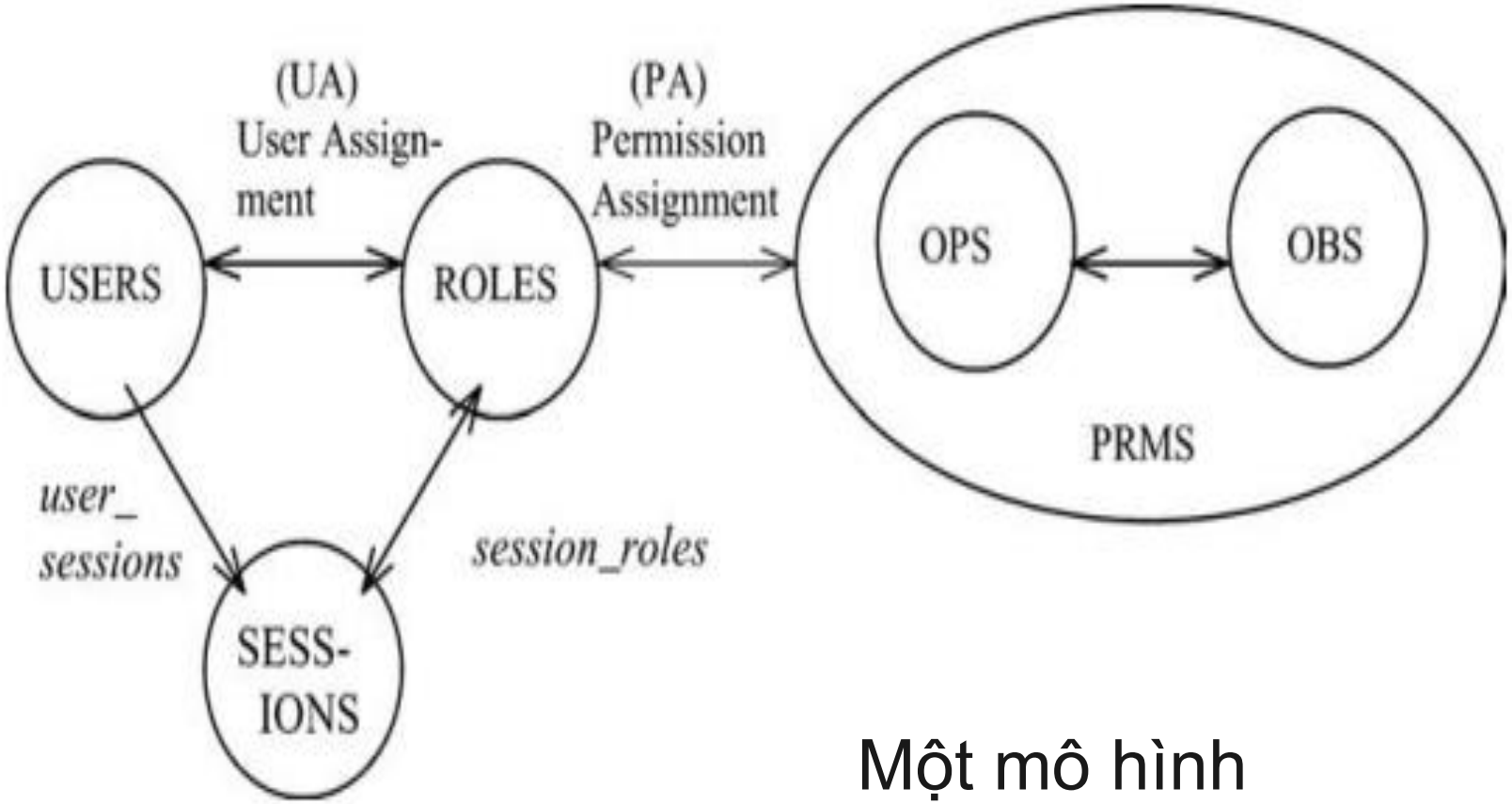
5.1.2 Các biện pháp điều khiển truy nhập - RBAC

- Ví dụ: một trường học chia người dùng thành các nhóm gán sẵn quyền truy nhập vào các phần trong hệ thống:
  - Nhóm Quản lý được quyền truy nhập vào tất cả các thông tin trong hệ thống;
  - Nhóm Giáo viên được truy nhập vào CSDL các môn học, bài báo khoa học, cập nhật điểm các lớp phụ trách;
  - Nhóm Sinh viên chỉ được quyền xem nội dung các môn học, tải tài liệu học tập và xem điểm của mình.

5.1.2 Các biện pháp điều khiển truy nhập - RBAC

- Liên kết giữa người dùng và vai trò:
  - Người dùng được cấp "thẻ thành viên" của các nhóm "vai trò" trên cơ sở năng lực và vai trò, cũng như trách nhiệm của họ trong một tổ chức.
- Trong nhóm "vai trò", người dùng được cấp vừa đủ quyền để thực hiện các thao tác cần thiết cho công việc được giao.
- Liên kết giữa người dùng và vai trò có thể được tạo lập và huỷ bỏ dễ dàng.
- Quản lý phân cấp vai trò: các vai trò được tổ chức thành một cây theo mô hình phân cấp tự nhiên của các công ty/tổ chức.

5.1.2 Các biện pháp điều khiển truy nhập - RBAC



Một mô hình RBAC đơn giản

5.1.2 Các biện pháp điều khiển truy nhập – Rule-Based AC

- Điều khiển truy nhập dựa trên luật cho phép người dùng truy nhập vào hệ thống và thông tin dựa trên các luật (rules) đã được định nghĩa trước.
- Các luật có thể được thiết lập để hệ thống cho phép truy nhập đến các tài nguyên của mình cho người dùng thuộc một tên miền, một mạng hay một dải địa chỉ IP.

5.1.2 Các biện pháp điều khiển truy nhập – Rule-Based AC

- Firewalls/Proxies là ví dụ điển hình về điều khiển truy nhập dựa trên luật:
  - Dựa trên địa chỉ IP nguồn và đích của các gói tin;
  - Dựa trên phần mở rộng các files để lọc các mã độc hại;
  - Dựa trên địa chỉ IP hoặc các tên miền để lọc/chặn các website bị cấm;
  - Dựa trên tập các từ khoá để lọc các nội dung bị cấm.

5.1.3 Một số công nghệ điều khiển truy nhập

- Điều khiển truy nhập dựa trên mật khẩu (password)
- Điều khiển truy nhập dựa trên các khoá mã (encrypted keys)
- Điều khiển truy nhập dựa trên thẻ thông minh (smart card)
- Điều khiển truy nhập dựa trên thẻ bài (token)
- Điều khiển truy nhập dựa trên các đặc điểm sinh trắc học (biometric).

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên mật khẩu

- Thông thường mỗi người dùng được cấp 1 tài khoản (account) để truy nhập vào hệ thống. Để truy nhập tài khoản, thường cần có:
  - Tên người dùng (username), email, số điện thoại...
  - Mật khẩu (Password)
    - Mật khẩu có thể ở dạng nguyên bản (plain text)
    - Mật khẩu có thể ở dạng mã hoá (encrypted text)
      - Các thuật toán thường dùng để mã hoá mật khẩu: MD4, MD5, SHA-1, SHA256,...
    - Mật khẩu có thể được dùng nhiều lần hoặc 1 lần (one time password).

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên mật khẩu

- Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên:
  - Độ khó đoán của mật khẩu
    - Dùng nhiều loại ký tự
      - Chữ thường, hoa, chữ số, ký tự đặc biệt:
        - abc1234: mật khẩu tồi
        - aBc*1#24: mật khẩu tốt (về mặt tính toán)
    - Độ dài của mật khẩu
      - Mật khẩu tốt có chiều dài >= 8 ký tự
  - Tuổi thọ của mật khẩu
    - Mật khẩu không hết hạn
    - Mật khẩu có thời hạn sống
    - Mật khẩu dùng 1 lần

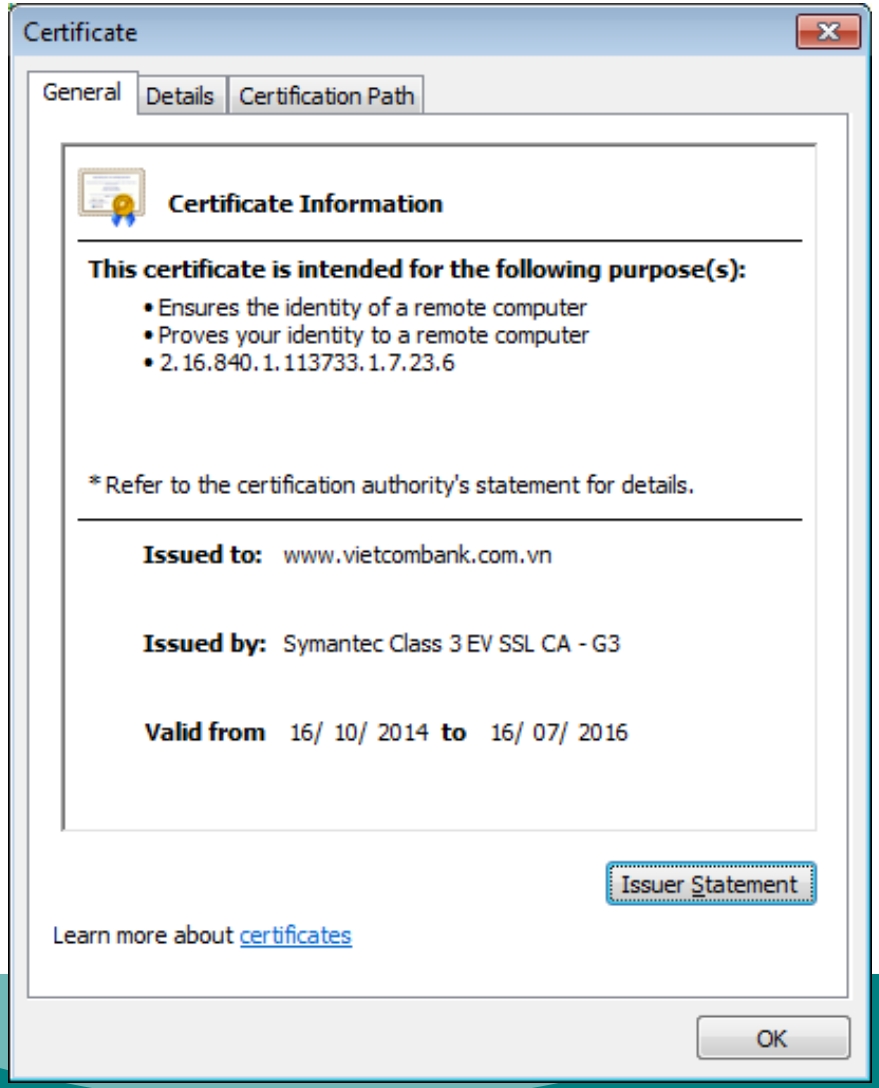
5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên mật khẩu

- Mật khẩu một lần (OTP-One Time Password):
  - Mật khẩu được sinh ra và chỉ được dùng 1 lần cho 1 phiên làm việc hoặc 1 giao dịch;
  - Mật khẩu thường được sinh ngẫu nhiên
  - Chuyển giao OTP:
    - In ra giấy một danh sách mật khẩu để dùng dần
    - Gửi qua các phương tiện khác như SMS
    - Sử dụng các thiết bị chuyên dụng, như các token,...
  - Ưu điểm: an toàn hơn, tránh được tấn công kiểu replay (lấy được mật khẩu dùng lại).
  - Nhược điểm: người sử dụng khó nhớ mật khẩu.

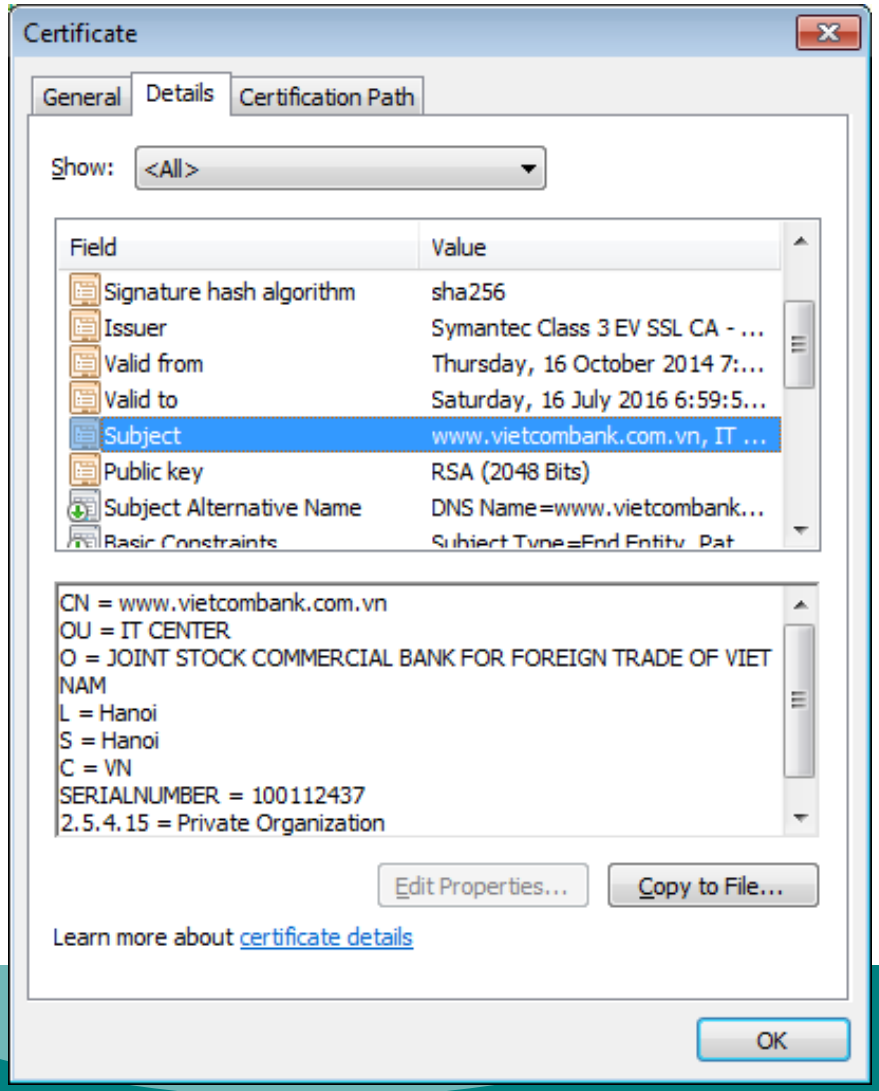
5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các khóa mã

- Khoá mã là các giải thuật cho phép:
  - Đảm bảo an toàn thông tin bí mật
  - Cho phép kiểm tra thông tin nhận dạng của các bên tham gia giao dịch.
- Ứng dụng rộng rãi nhất là chứng chỉ số (Digital Certificate). Một chứng chỉ số thường gồm:
  - Thông tin nhận dạng của chủ thể
  - Khoá công khai của chủ thể
  - Các thông tin nhận dạng và khoá công khai của chủ thể được mã hoá (ký) bởi một tổ chức có thẩm quyền (Certificate Authority – CA).

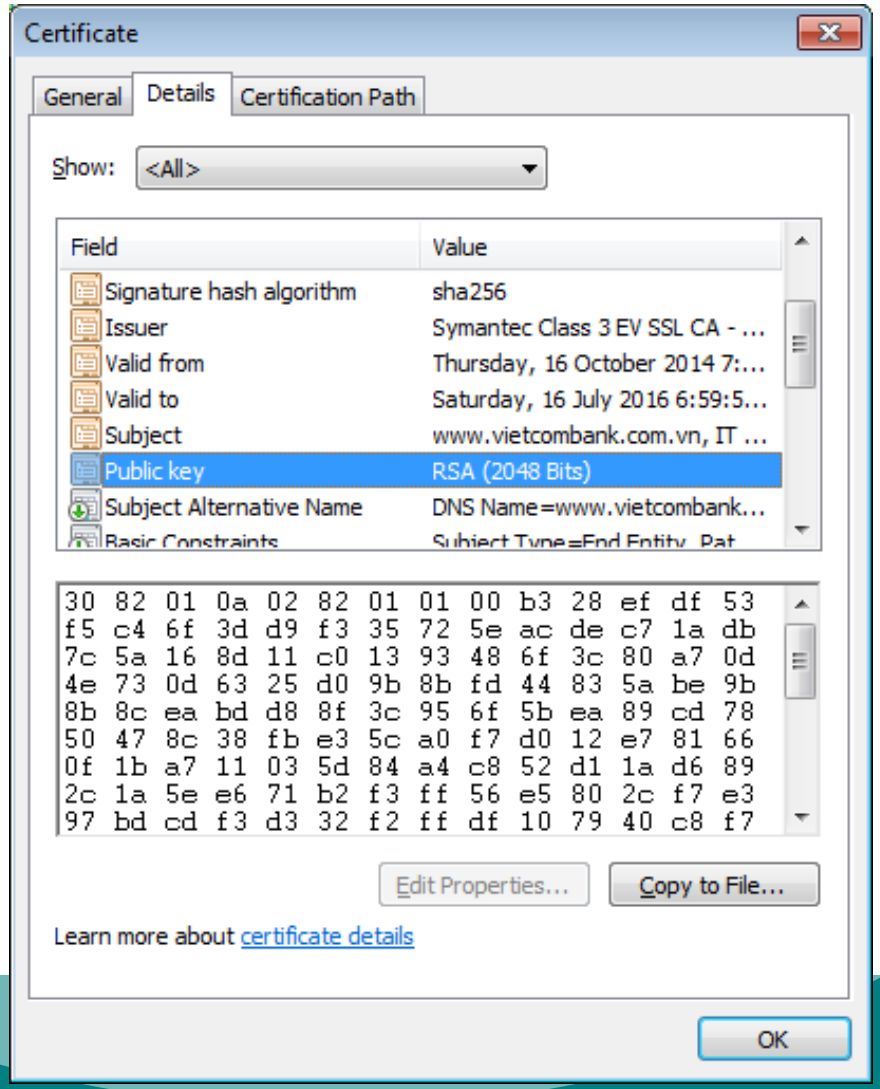
5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các khóa mã



5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các khóa mã



5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các khóa mã



5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ thông minh

- Thẻ thông minh (Smartcard) là các thẻ nhựa có gắn các chip điện tử
- Có khả năng tính toán và các thông tin lưu trong thẻ được mã hoá
- Smartcard sử dụng hai yếu tố (two-factors) để xác thực và nhận dạng chủ thể:
  - Cái bạn có (what you have): thẻ
  - Cái bạn biết (what you know): số PIN

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ thông minh

Một loại thẻ thông minh (thẻ tiếp xúc)

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ thông minh

Một loại thẻ thông minh (thẻ không tiếp xúc)

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ bài (token)

- Các thẻ bài thường là các thiết bị cầm tay được thiết kế nhỏ gọn để có thể dễ dàng mang theo;
  - Được tích hợp pin cung cấp nguồn nuôi.
- Thẻ bài có thể được sử dụng để lưu:
  - Mật khẩu
  - Thông tin cá nhân
  - Các thông tin khác

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ bài (token)

- Thẻ bài thường được trang bị cơ chế xác thực 2 yếu tố tương tự smartcards:
  - Thẻ bài
  - Mật khẩu (thường dùng 1 lần)
- Thẻ bài thường có cơ chế xác thực mạnh hơn smartcards do năng lực tính toán cao hơn:
  - CPU có năng lực xử lý cao hơn smartcard;
  - Bộ nhớ lưu trữ lớn hơn.

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ bài (token)

Thẻ bài (token) của hãng RSA Security

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

RSA SecurID SID800

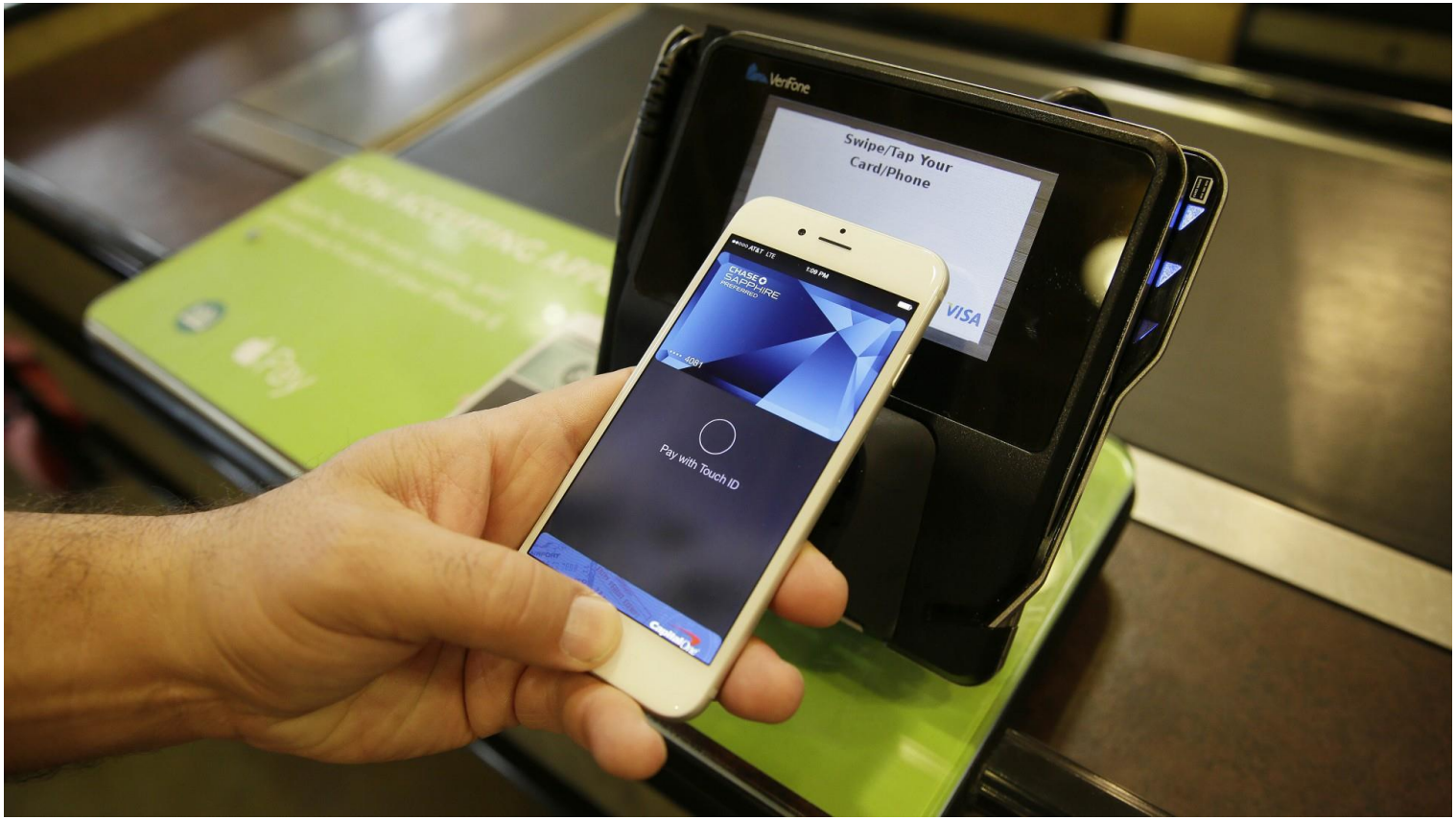
RSA SecurID SD520

BlackBerry with
RSA SecurID software token

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ bài (token)

Thẻ bài (ví điện tử) của PayPal dùng trong thanh toán trực tuyến

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên thẻ bài (token)



5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

- Điều khiển truy nhập có thể sử dụng các đặc điểm sinh trắc học để nhận dạng chủ thể:
  - Dấu vân tay
  - Tròng mắt
  - Khuôn mặt
  - Tiếng nói
  - Chữ ký tay

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

- Ưu điểm:
  - Có khả năng bảo mật cao
  - Luôn đi cùng chủ thể
- Nhược điểm:
  - Chi phí đắt
  - Chậm do đòi hỏi khối lượng tính toán lớn
  - Tỷ lệ nhận dạng sai tương đối lớn do có nhiều yếu tố ảnh hưởng.

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

Khoá sử dụng vân tay

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

Khoá sử dụng vân tay

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

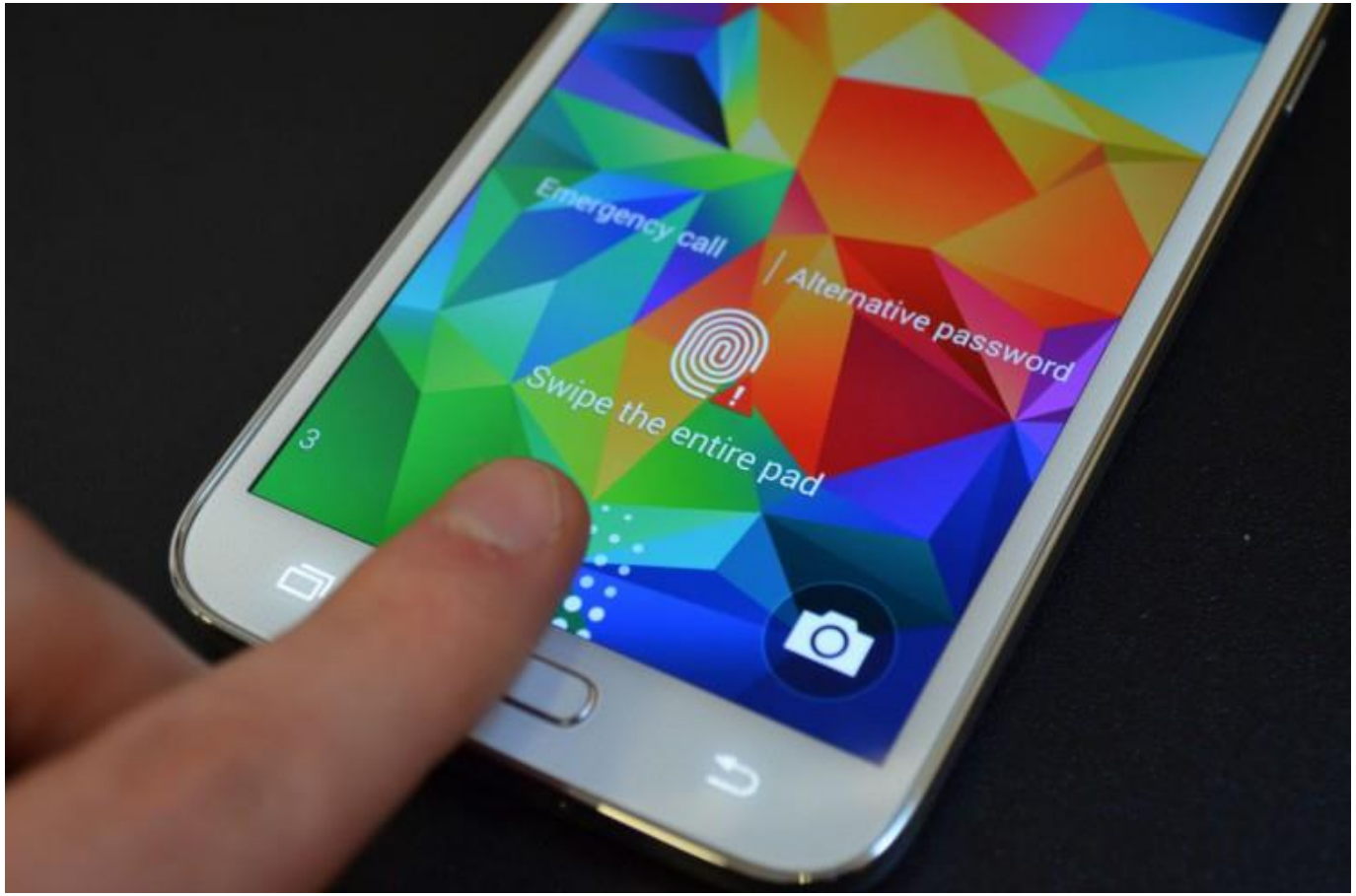
Bộ phận đọc vân tay trên laptop

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

Bộ phận đọc vân tay trên điện thoại iPhone

5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

Bộ phận đọc vân tay trên điện thoại Samsung



5.1.3 Một số công nghệ điều khiển truy nhập – Điều khiển truy nhập dựa trên các đặc điểm sinh học

Bộ phận quét nhận dạng mắt/ con ngươi

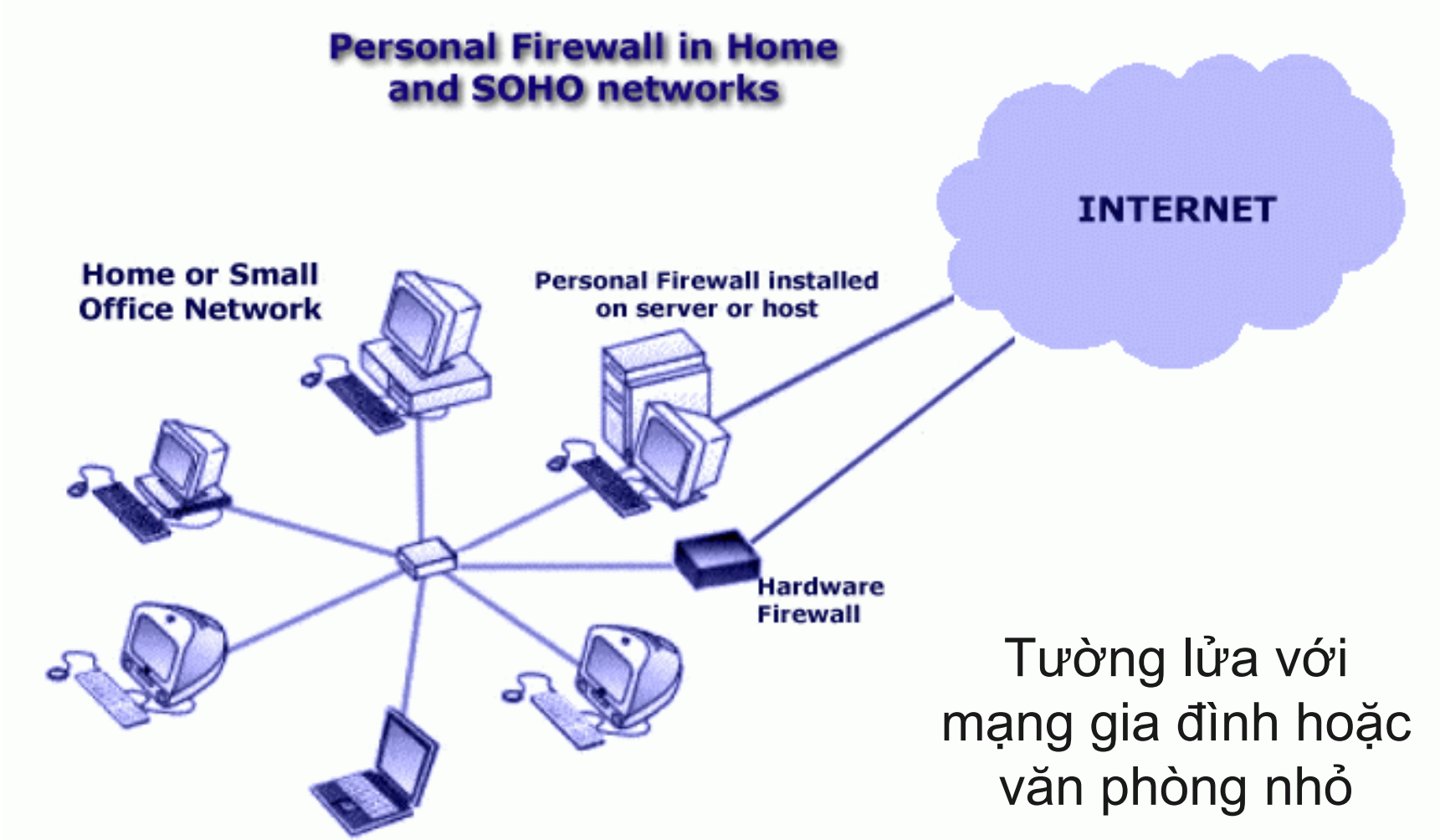
5.2 Tường lửa – Giới thiệu

- Tường lửa (firewall) có thể dùng để bảo hệ thống và mạng cục bộ tránh các đe doạ từ bên ngoài.
- Tường lửa thường được đặt ở vị trí cổng vào của mạng nội bộ công ty hoặc tổ chức.

5.2 Tường lửa – Giới thiệu

- Tất cả các gói tin từ trong ra và từ ngoài vào đều phải đi qua tường lửa.
- Chỉ các gói tin hợp lệ được phép đi qua tường lửa (xác định bởi chính sách an ninh).
- Bản thân tường lửa phải miễn dịch với các loại tấn công.
- Tường lửa có thể ngăn chặn nhiều hình thức tấn công mạng, như IP spoofing.

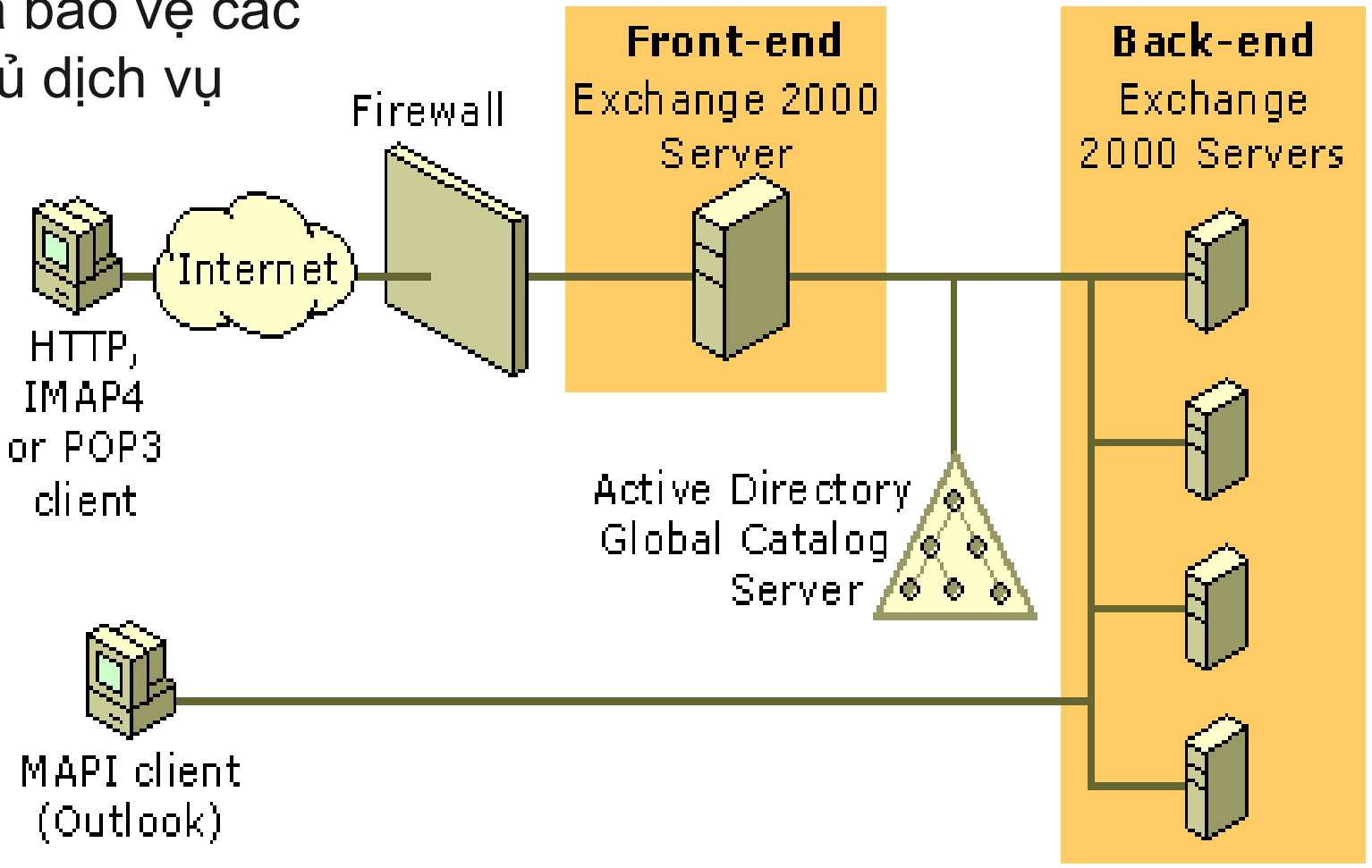
5.2 Tường lửa – Tôpô mạng với tường lửa



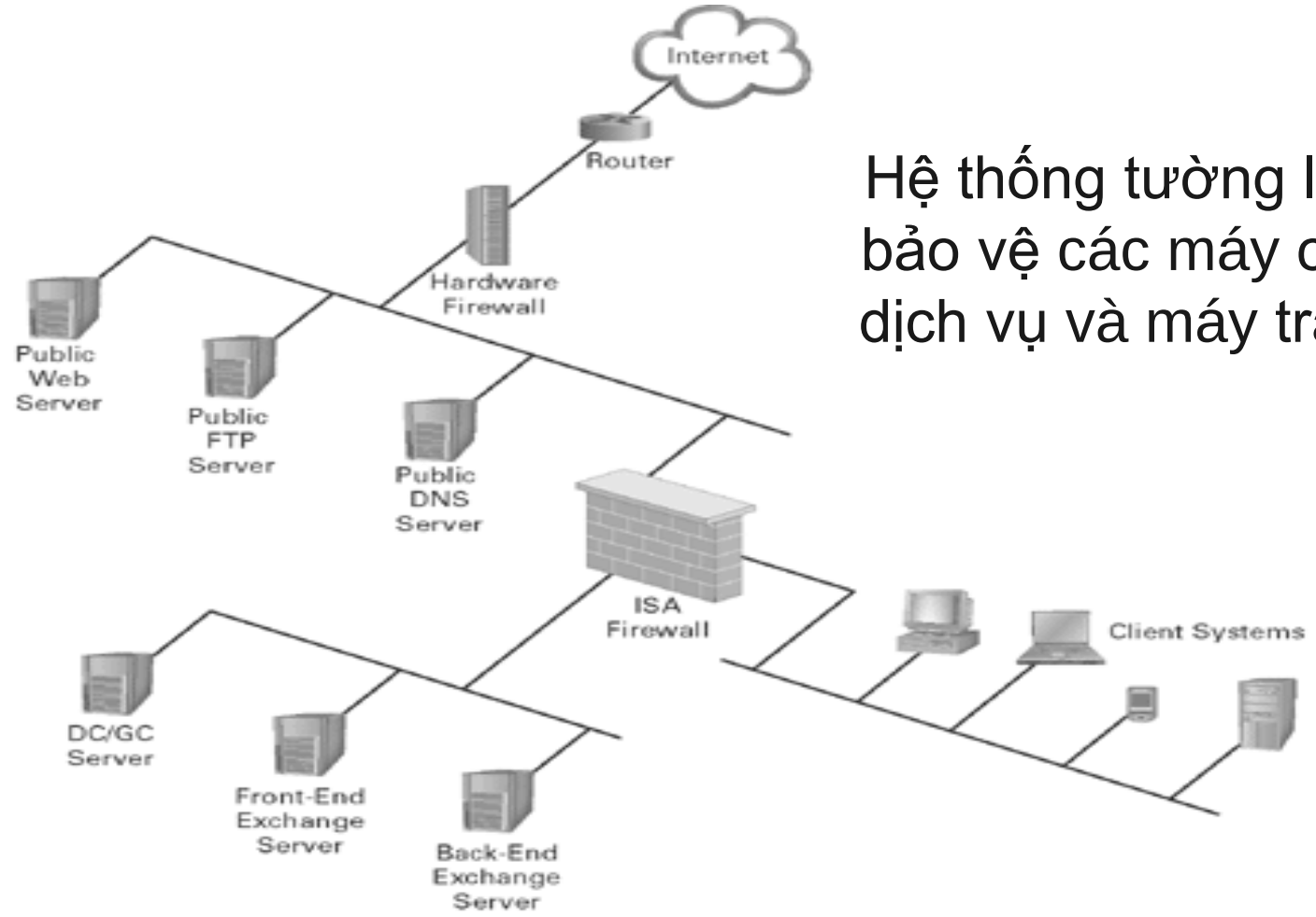
Tường lửa với mạng gia đình hoặc văn phòng nhỏ

5.2 Tường lửa – Tôpô mạng với tường lửa

Tường lửa bảo vệ các máy chủ dịch vụ



5.2 Tường lửa – Tôpô mạng với tường lửa



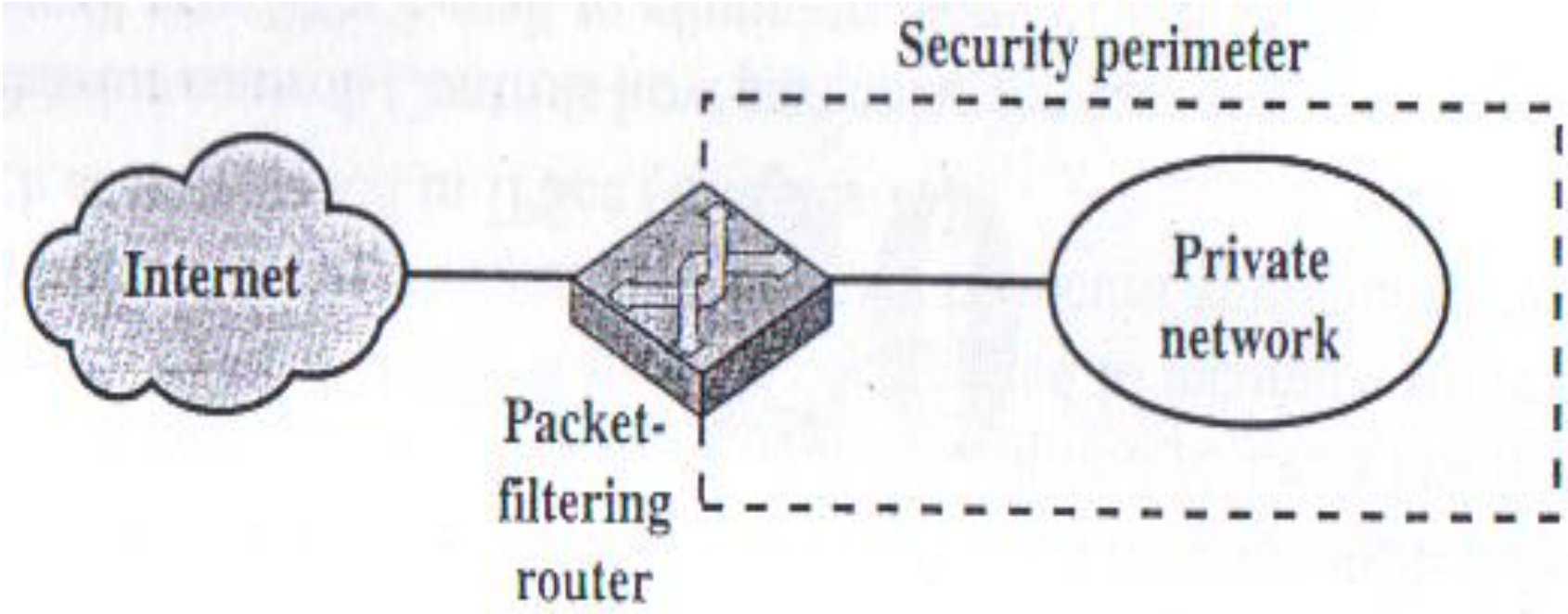
Back-to-back firewall network protecting an OWA Web site.

Hệ thống tường lửa bảo vệ các máy chủ dịch vụ và máy trạm

5.2 Tường lửa – Các loại tường lửa

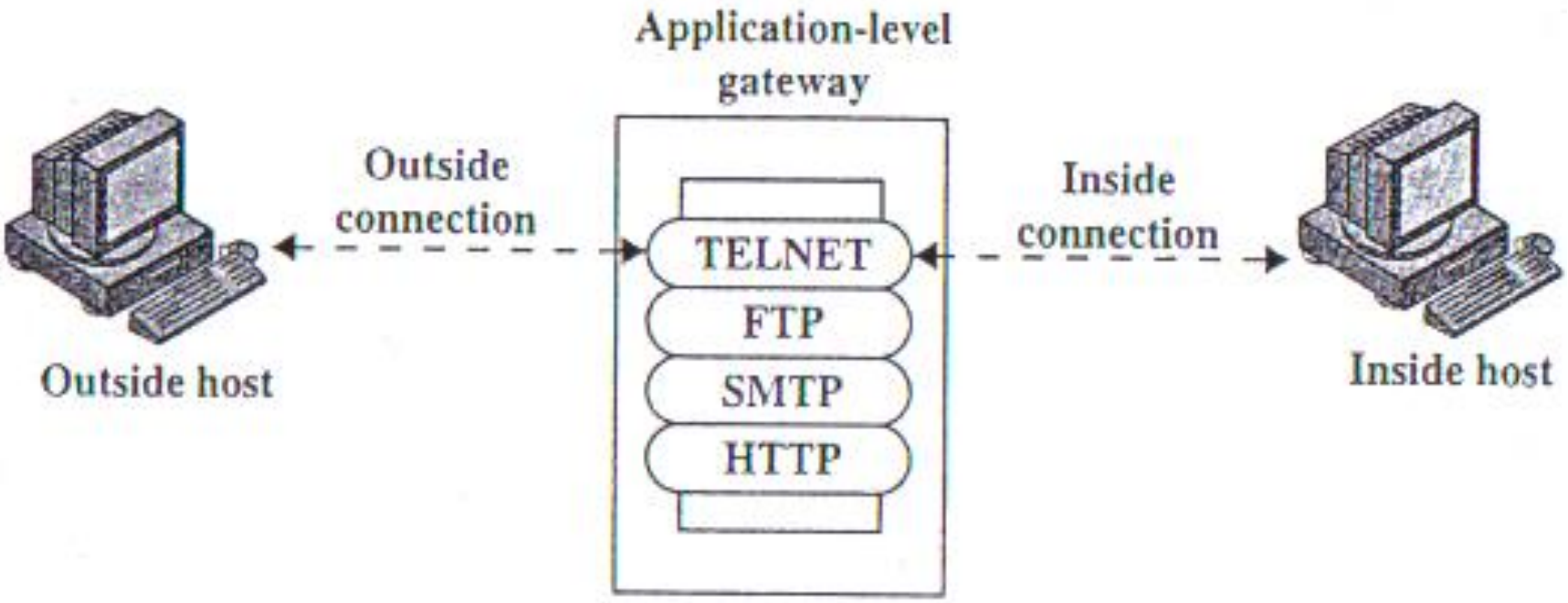
- Lọc gói tin (Packet-Filtering):
  - Áp dụng một tập các luật cho mỗi gói tin đi/đến để quyết định chuyển tiếp hay loại bỏ gói tin.
- Các cổng ứng dụng (Application-level gateway):
  - Còn gọi là proxy server, thường dùng để phát lại (relay) traffic của mức ứng dụng.
- Cổng chuyển mạch (Circuit-level gateway):
  - Hoạt động tương tự các bộ chuyển mạch.

5.2 Tường lửa – Các loại tường lửa – Lọc gói tin



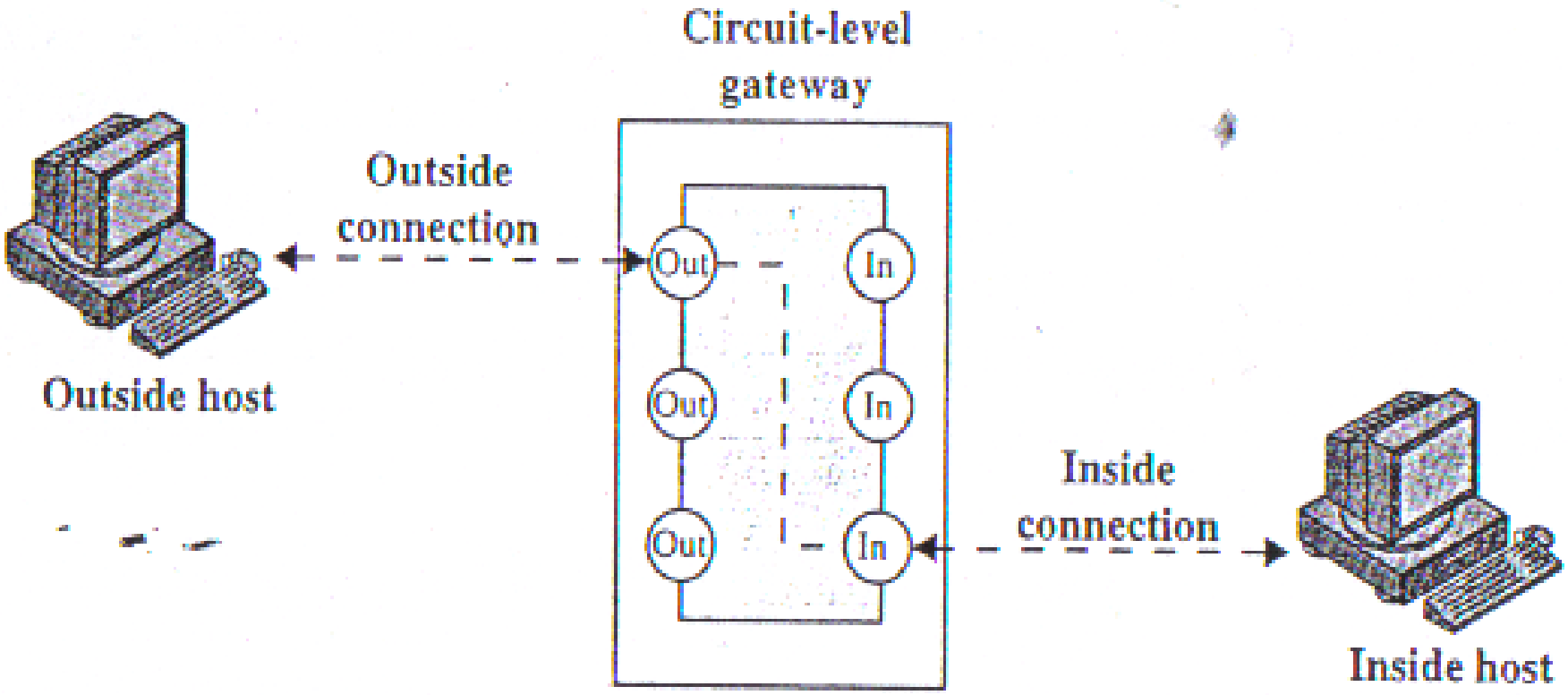
(a) Packet-filtering router

5.2 Tường lửa – Các loại tường lửa – Cổng ứng dụng



(b) Application-level gateway

5.2 Tường lửa – Các loại tường lửa – Cổng chuyển mạch

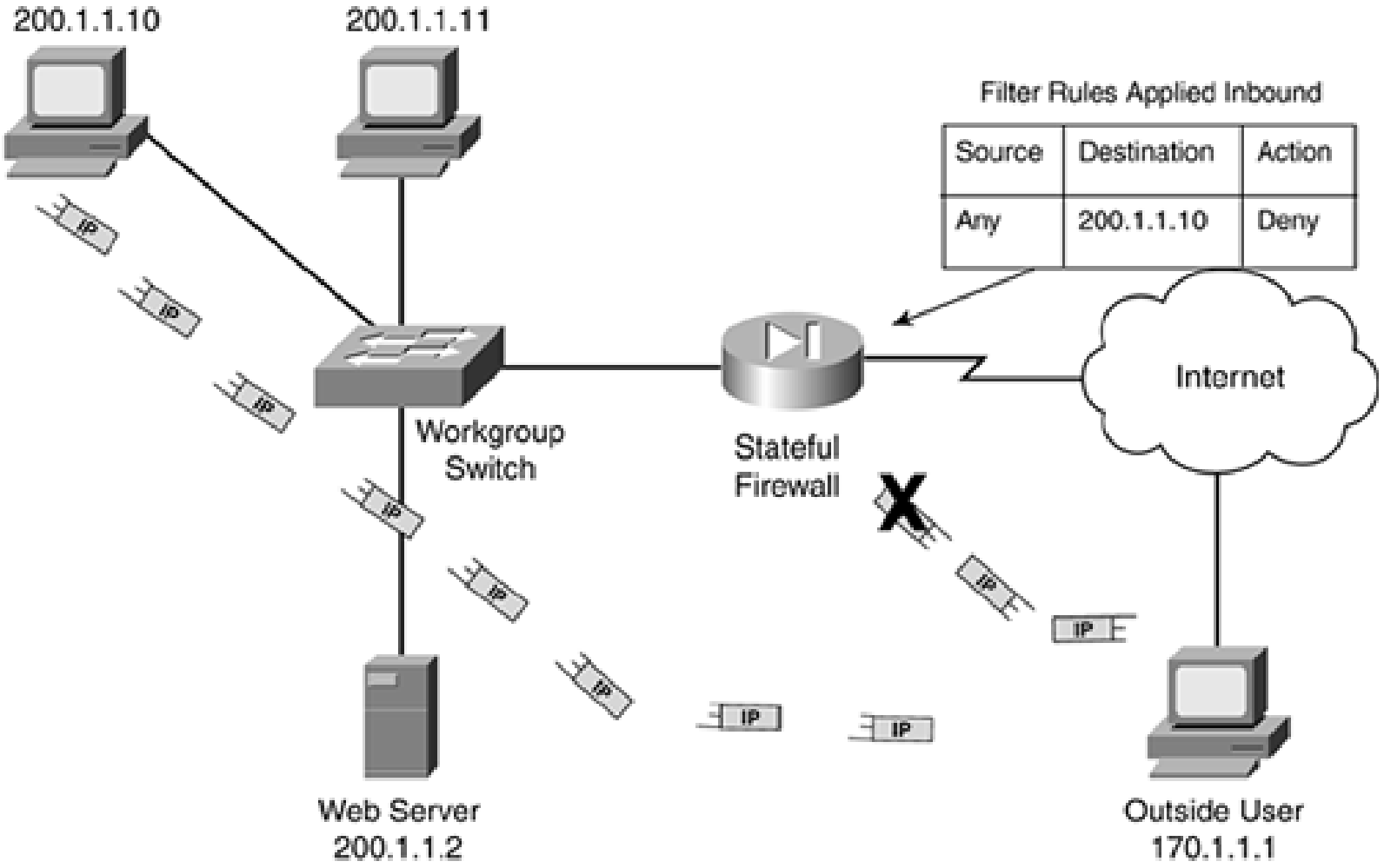


(c) Circuit-level gateway

5.2 Tường lửa – Lọc có trạng thái

- Tường lửa có trạng thái (Stateful firewall):
  - Có khả năng lưu trạng thái của các kết nối mạng đi qua nó;
  - Nó được lập trình để phân biệt các gói tin thuộc về các kết nối mạng khác nhau;
  - Chỉ những gói tin thuộc một kết nối mạng đang hoạt động mới được đi qua tường lửa, còn các gói tin khác (không thuộc kết nối đang hoạt động) sẽ bị chặn lại.

5.2 Tường lửa – Lọc có trạng thái và không trạng thái



5.2 Tường lửa – Lọc không trạng thái

- Tường lửa không trạng thái (Stateless firewall):
  - Lọc các gói tin riêng rẽ mà không quan tâm đến mỗi gói tin thuộc về kết nối mạng nào;
  - Dễ bị tấn công bởi kỹ thuật giả mạo địa chỉ, giả mạo nội dung gói tin do tường lửa không có khả năng nhớ các gói tin đi trước thuộc cùng một kết nối mạng.

5.2 Tường lửa – Kỹ thuật kiểm soát truy nhập

- Kiểm soát dịch vụ:
  - Xác định dịch vụ nào có thể được truy nhập, hướng đi ra hay đi vào.
- Kiểm soát hướng:
  - Điều khiển hướng được phép đi của các gói tin của mỗi dịch vụ
- Kiểm soát người dùng:
  - Xác định người dùng nào được quyền truy nhập;
  - Thường áp dụng cho người dùng mạng nội bộ.
- Kiểm soát hành vi:
  - Kiểm soát việc sử dụng các dịch vụ cụ thể. Ví dụ: tường lửa có thể lọc để loại bỏ các thư rác, hoặc hạn chế truy nhập đến một bộ phận thông tin của máy chủ web.

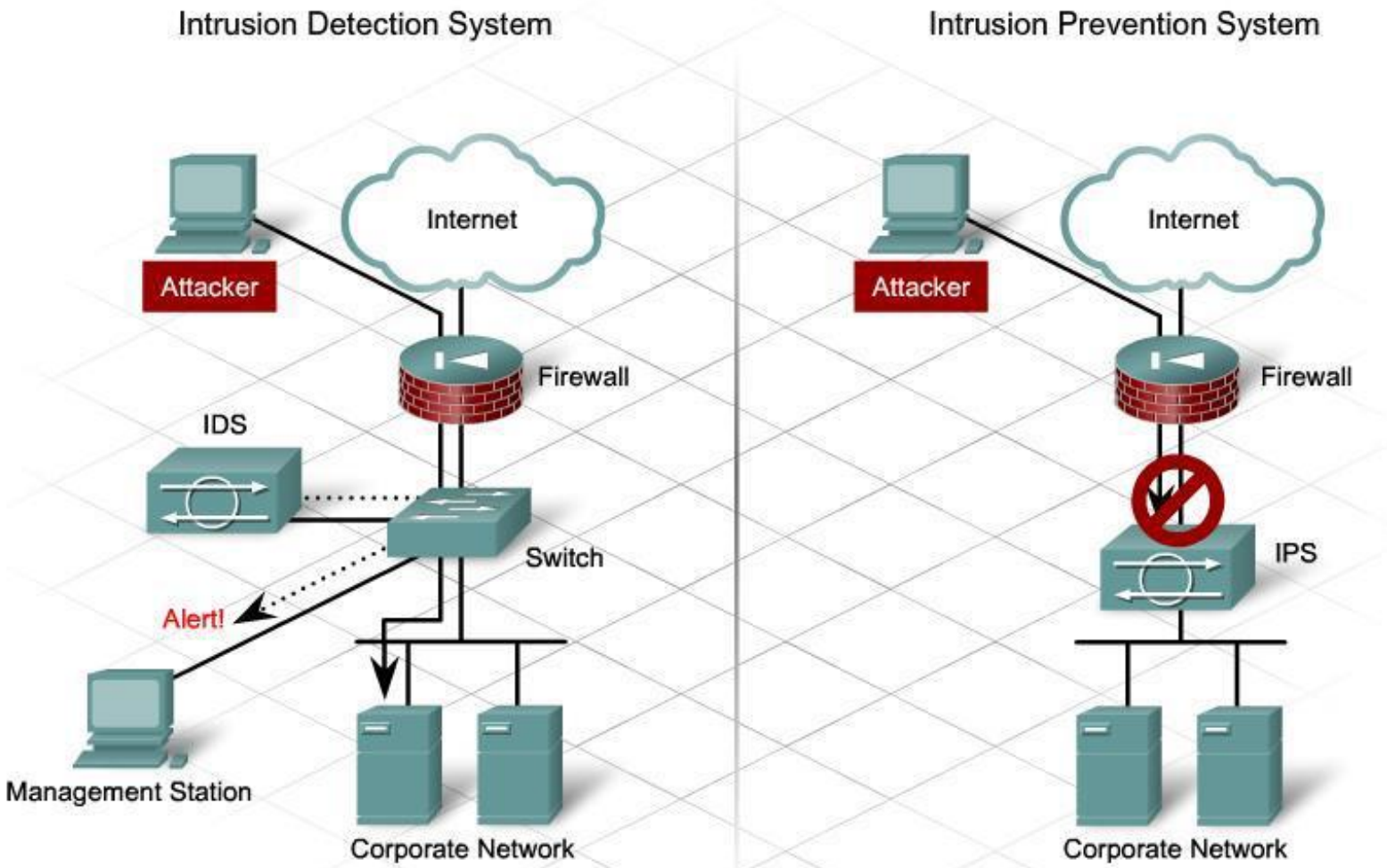
5.2 Tường lửa – Các hạn chế

- Không thể chống lại các tấn công không đi qua nó.
- Không thể chống lại các tấn công hướng dữ liệu, hoặc tấn công vào các lỗ hổng an ninh của các phần mềm.
- Không thể chống lại các hiểm hoạ từ bên trong (mạng nội bộ).
- Không thể ngăn chặn việc vận chuyển các chương trình hoặc các file bị nhiễm virus hoặc các phần mềm độc hại.

5.3 Các hệ thống ngăn chặn/phát hiện tấn công, đột nhập

- Các hệ thống phát hiện/ngăn chặn tấn công, đột nhập (IDS/IPS) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng;
  - IDS – Intrusion Detection System: hệ thống phát hiện tấn công, đột nhập;
  - IPS - Intrusion Prevention System: hệ thống ngăn chặn tấn công, đột nhập.
- Các hệ thống IDS/IPS có thể được đặt trước hoặc sau tường lửa, tùy theo mục đích sử dụng.

5.3 Các hệ thống ngăn chặn/phát hiện tấn công, đột nhập



5.3 Các hệ thống ngăn chặn/phát hiện tấn công, đột nhập

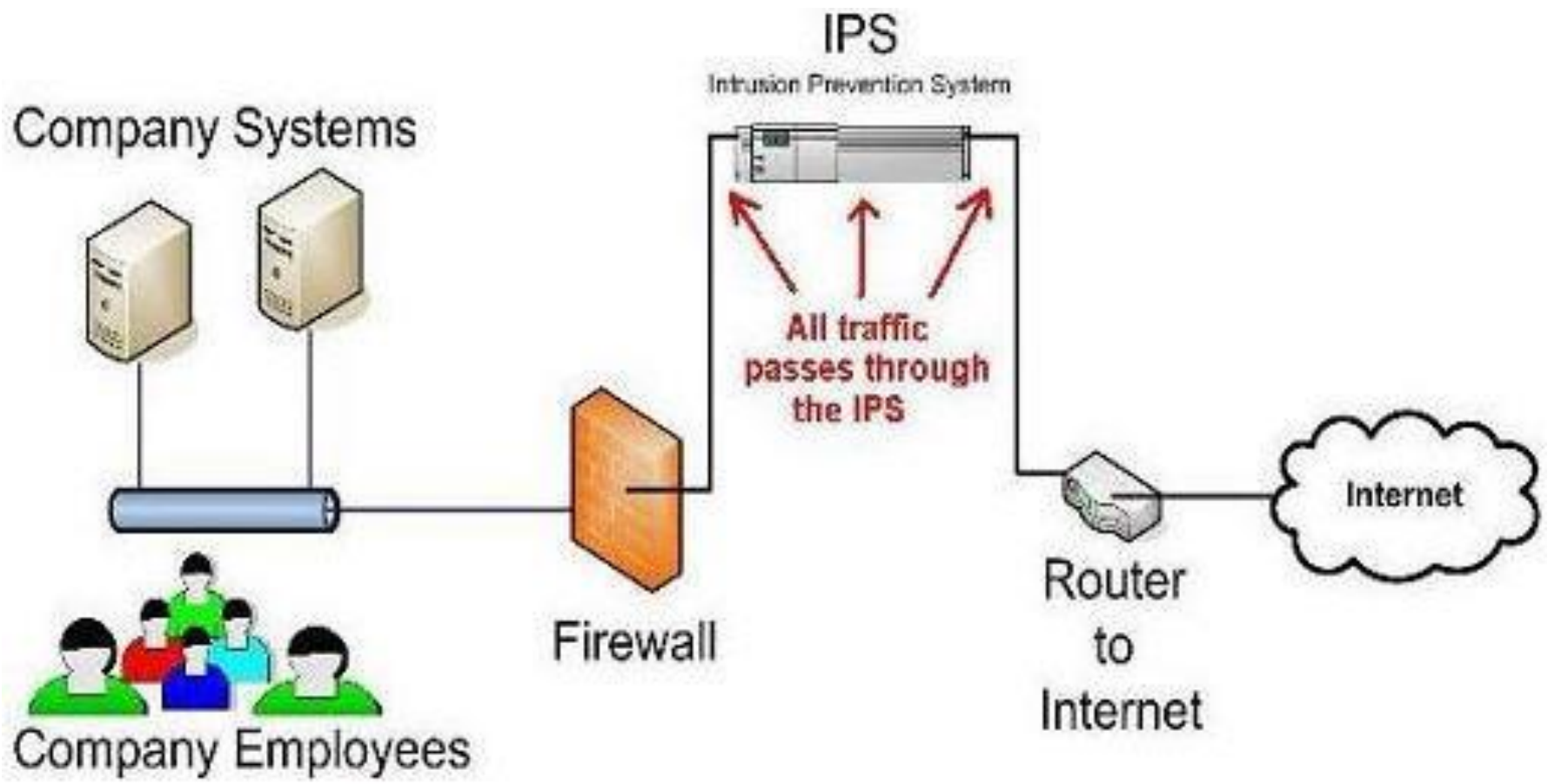
- Nhiệm vụ chính của các hệ thống IDS/IPS:
  - Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, đột nhập;
  - Khi phát hiện các hành vi tấn công, đột nhập → ghi logs các hành vi này cho phân tích bổ sung sau này;
  - Ngăn chặn hoặc dừng các hành vi tấn công, đột nhập;
  - Gửi thông báo cho người quản trị về các các hành vi tấn công, đột nhập đã phát hiện được.

5.3 Các hệ thống ngăn chặn/phát hiện tấn công, đột nhập

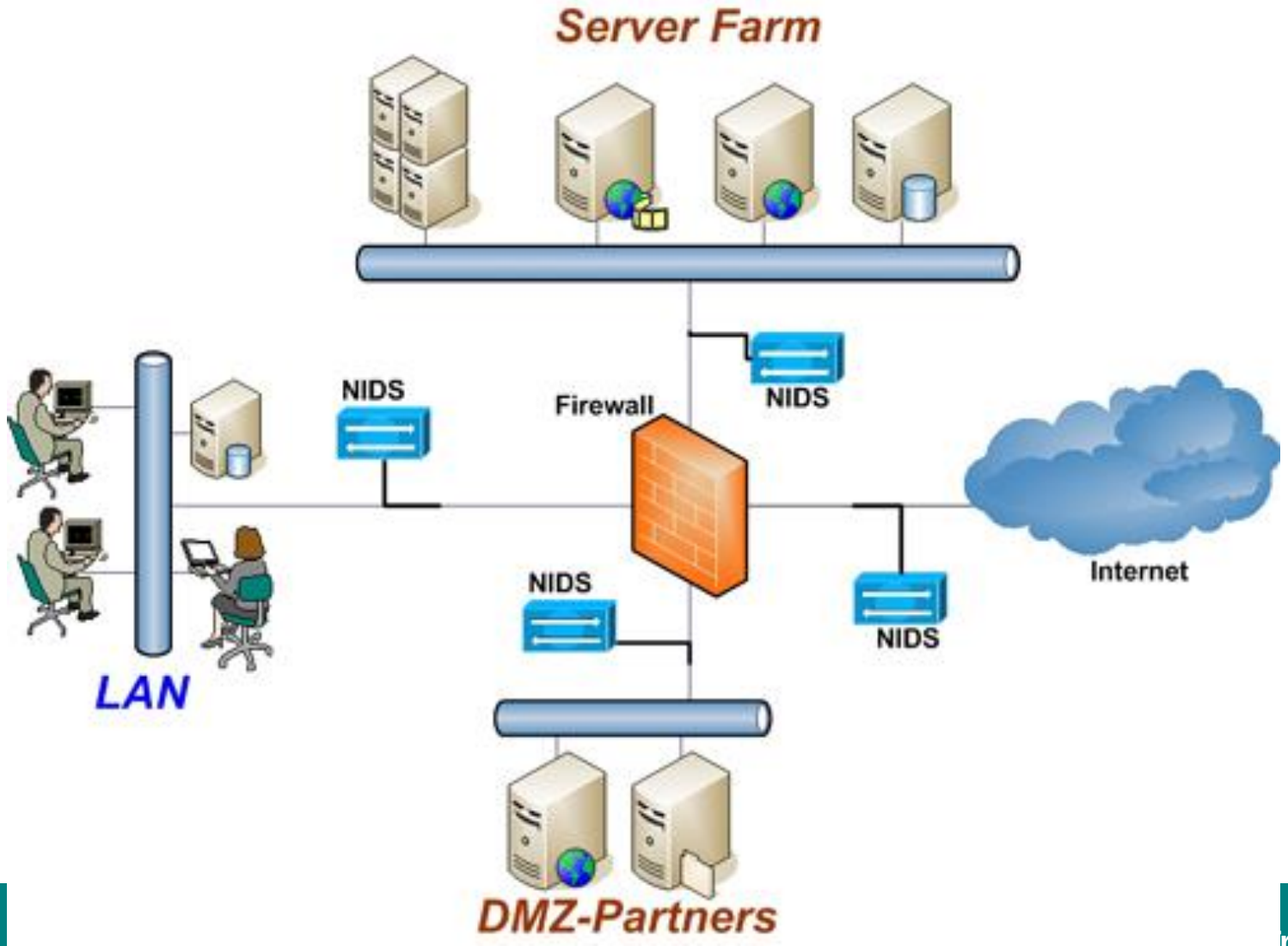
❖So sánh IDS/IPS:

- Giống: Về cơ bản IPS và IDS giống nhau về chức năng giám sát.
- Khác:
  - IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công/đột nhập bị phát hiện;
  - IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát/cảnh bảo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

5.3 Các hệ thống ngăn chặn/phát hiện tấn công, đột nhập



5.3 Các hệ thống ngăn chặn/phát hiện tấn công, đột nhập



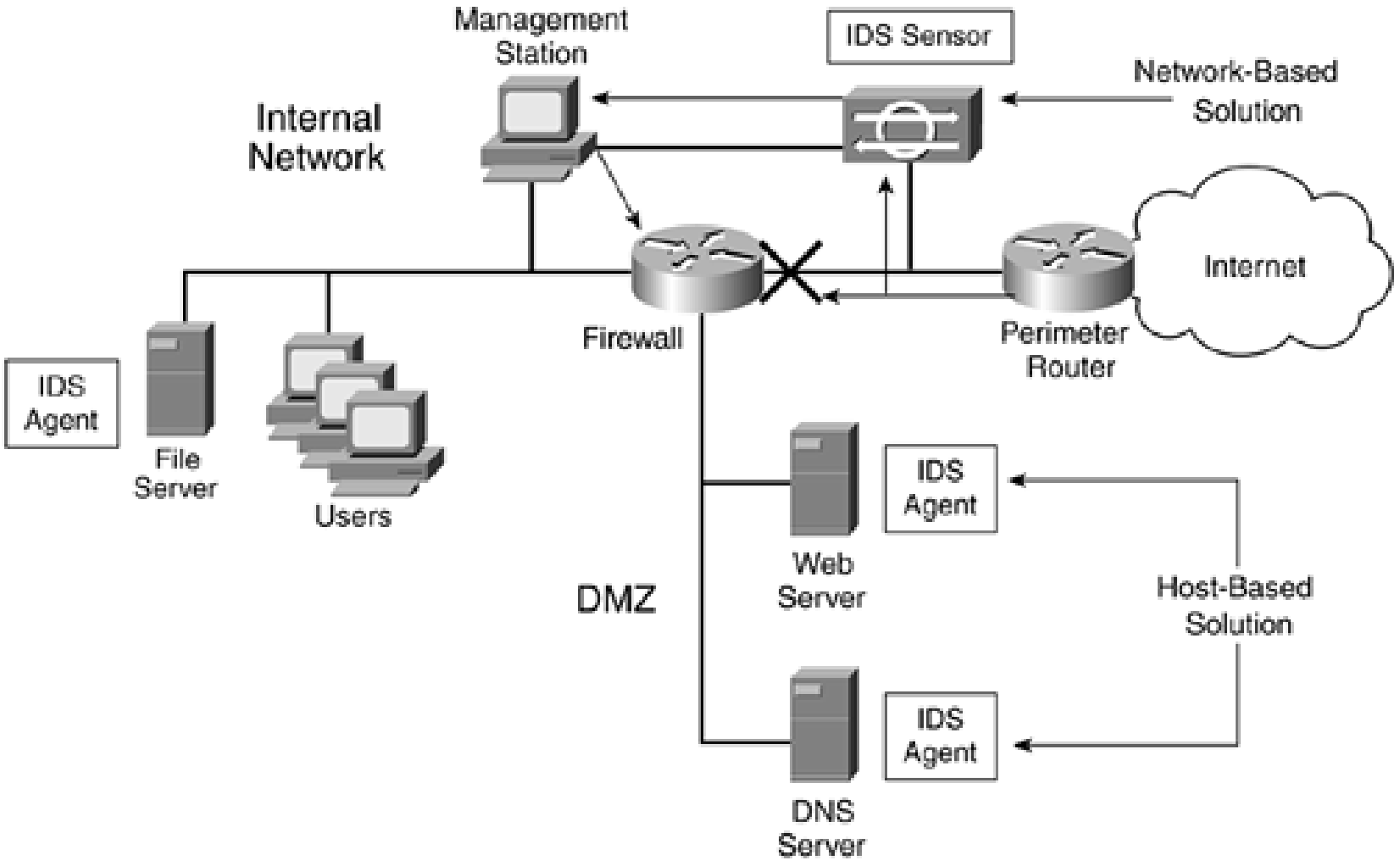
5.3 IDS/IPS – Phân loại

- Phân loại theo nguồn dữ liệu:
  - Hệ thống phát hiện đột nhập mạng (NIDS – Network-based IDS): phân tích lưu lượng mạng để phát hiện tấn công, đột nhập cho cả mạng hoặc một phần mạng.
  - Hệ thống phát hiện đột nhập cho host (HIDS – Host-based IDS): phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, đột nhập cho hệ thống đó.

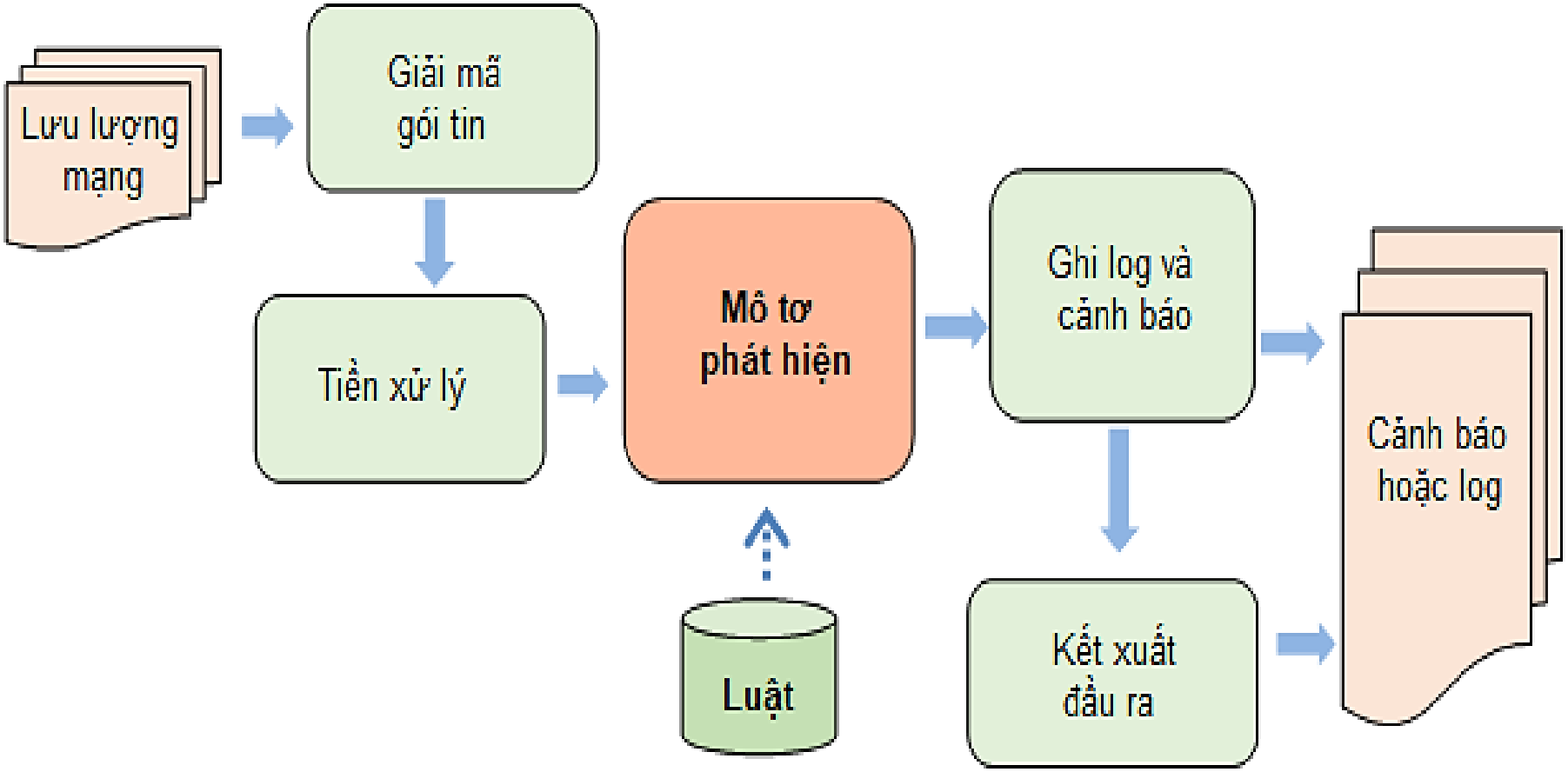
5.3 IDS/IPS – Phân loại

- Phân loại theo kỹ thuật phân tích:
  - Phát hiện đột nhập dựa trên chữ ký hoặc phát hiện sự lạm dụng (Signature-based / misuse instrusion detection);
  - Phát hiện đột nhập dựa trên các bất thường (Anomaly instrusion detection).

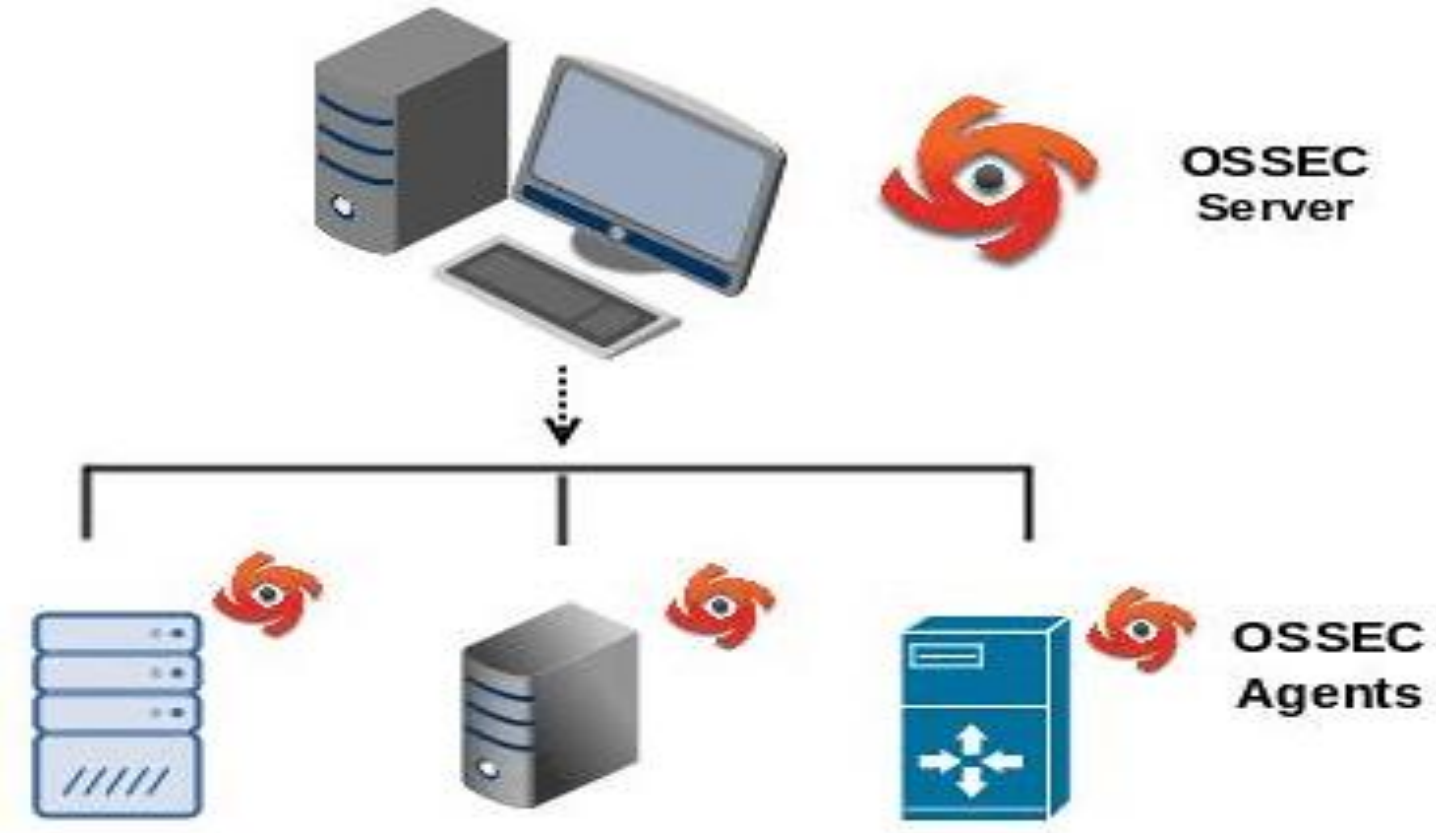
5.3 IDS/IPS – NIDS và HIDS



NIDS - Snort


Lưu lượng mạng
Giải mã gói tin
Tiền xử lý
Mô tơ phát hiện
Luật
Ghi log và cảnh báo
Kết xuất đầu ra
Cảnh báo hoặc log

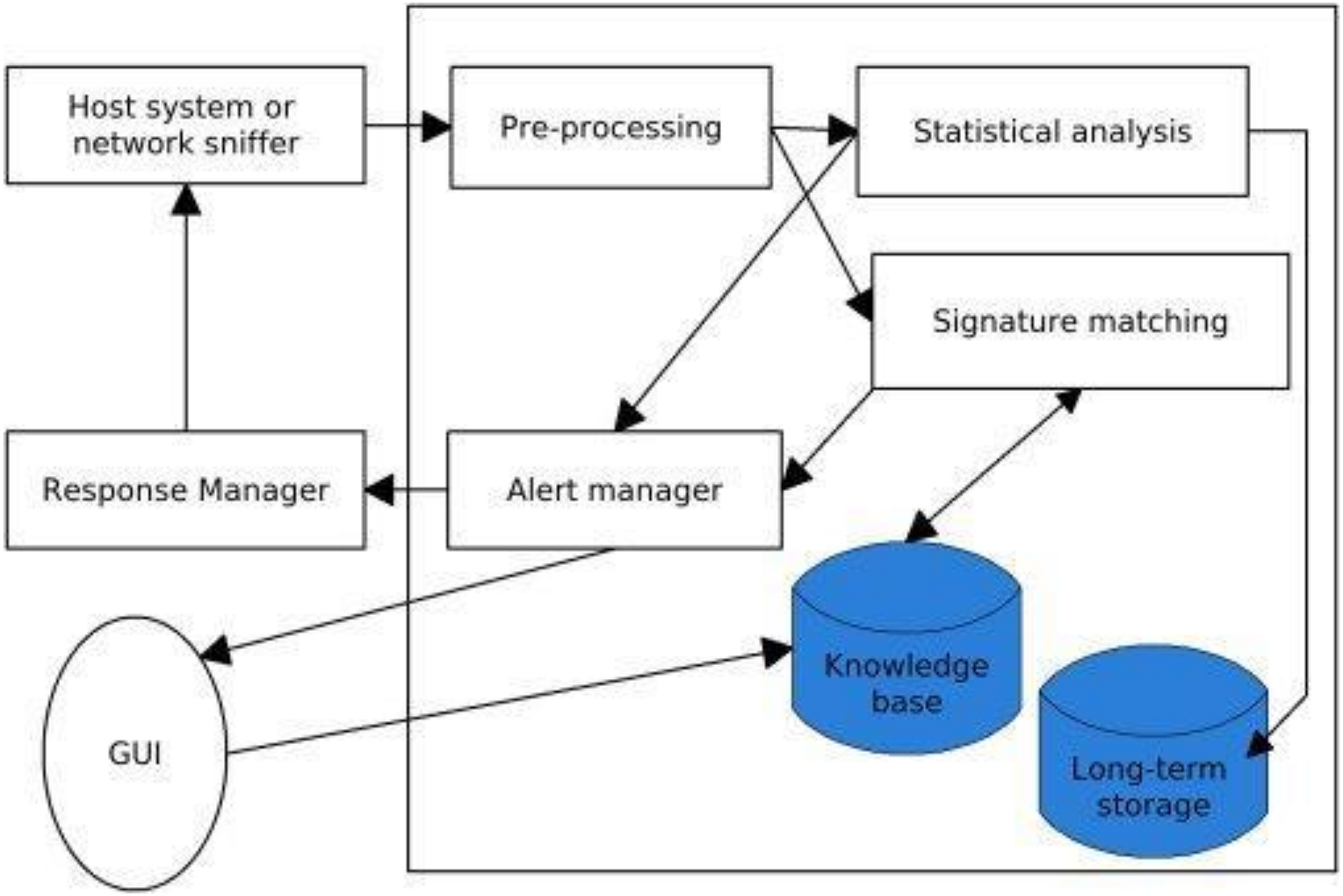
HIDS - OSSEC



5.3 IDS/IPS – Phát hiện đột nhập dựa trên chữ ký

- Xây dựng cơ sở dữ liệu các chữ ký/dấu hiệu của các loại tấn công, đột nhập đã biết;
  - Hầu hết các chữ ký/dấu hiệu được nhận dạng và mã hóa thủ công;
  - Dạng biểu diễn thường gặp là các luật (rule) phát hiện.
- Giám sát sát các hành vi của hệ thống, và cảnh báo nếu phát hiện chữ ký của tấn công, đột nhập;

5.3 IDS/IPS – Phát hiện đột nhập dựa trên chữ ký



5.3 IDS/IPS – Phát hiện đột nhập dựa trên chữ ký

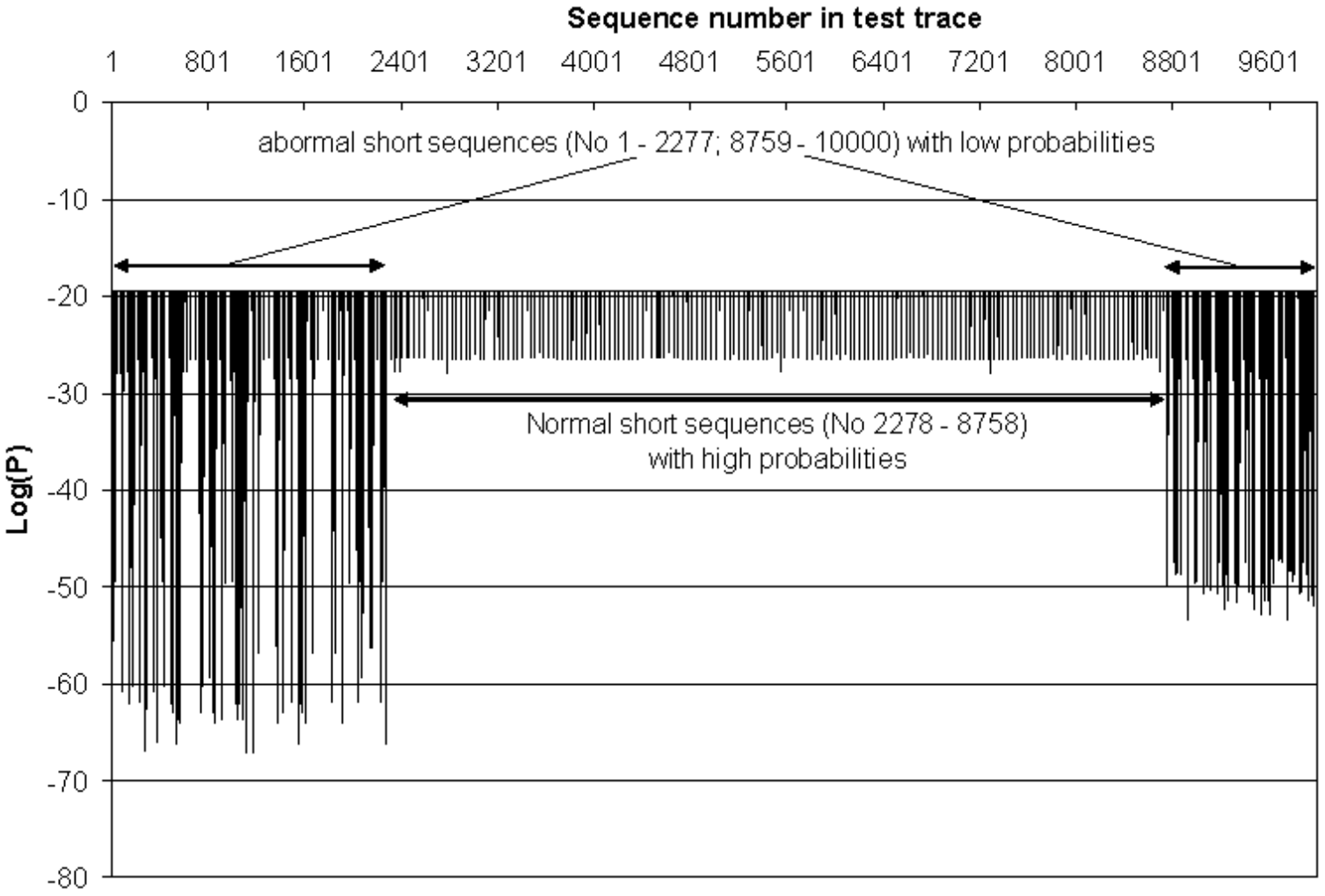
- Ưu điểm:
  - Có khả năng phát hiện các tấn công, đột nhập đã biết một cách hiệu quả;
  - Tốc độ cao, yêu cầu tài nguyên tính toán tương đối thấp.
- Nhược điểm:
  - Không có khả năng phát hiện các tấn công, đột nhập mới, do chữ ký của chúng chưa có trong cơ sở dữ liệu các chữ ký;
  - Đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký/dấu hiệu tấn công, xâm nhập.

5.3 IDS/IPS – Phát hiện đột nhập dựa trên bất thường

- Phương pháp này dựa trên giả thiết: *các hành vi đột nhập thường có quan hệ chặt chẽ với các hành vi bất thường*.
- Quá trình xây dựng và triển khai gồm 2 giai đoạn:
  - Xây dựng hồ sơ (profile) của đối tượng trong chế độ làm việc bình thường.
    - Cần giám sát đối tượng trong điều kiện bình thường trong một khoảng thời gian đủ dài để thu thập dữ liệu huấn luyện.
  - Giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và hồ sơ của đối tượng.

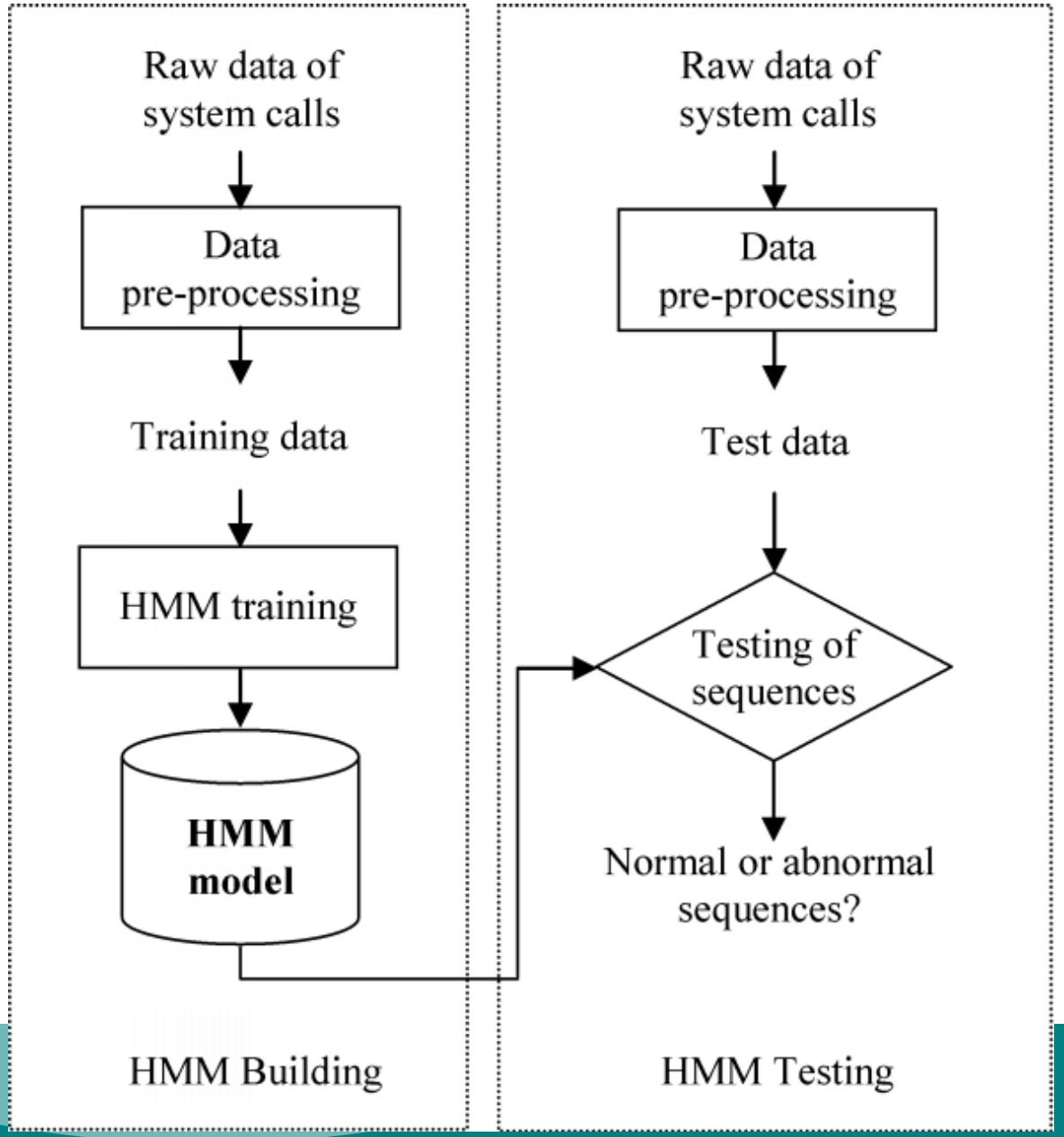
5.3 IDS/IPS – Phát hiện đột nhập dựa trên bất thường

Một ví dụ về tình trạng bình thường (Log(P) lớn) và bất thường (Log(P) rất nhỏ)



5.3 IDS/IPS – Phát hiện đột nhập dựa trên bất thường

HMM-Based Anomaly Detection



5.3 IDS/IPS – Phát hiện đột nhập dựa trên bất thường

- Ưu điểm:
  - Có tiềm năng phát hiện các loại đột nhập mới mà không yêu cầu biết trước thông tin về chúng.
- Nhược điểm:
  - Tỷ lệ cảnh báo sai tương đối cao so với phương pháp dựa trên chữ ký;
  - Tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.

5.3 IDS/IPS – Phát hiện đột nhập dựa trên bất thường

- Các phương pháp xử lý, phân tích dữ liệu và mô hình hoá trong phát hiện đột nhập dựa trên bất thường:
  - Thống kê (statistics).
  - Học máy (machine learning): HMM, máy trạng thái (state-based).
  - Khai phá dữ liệu (data mining).
  - Mạng nơ ron (neural networks).