TRƯỜNG ĐẠI HỌC NGUYỄN TẤT THÀNH
KHOA CÔNG NGHỆ THÔNG TIN

Bài giảng môn học: AN TOÀN THÔNG TIN

Chương 7:

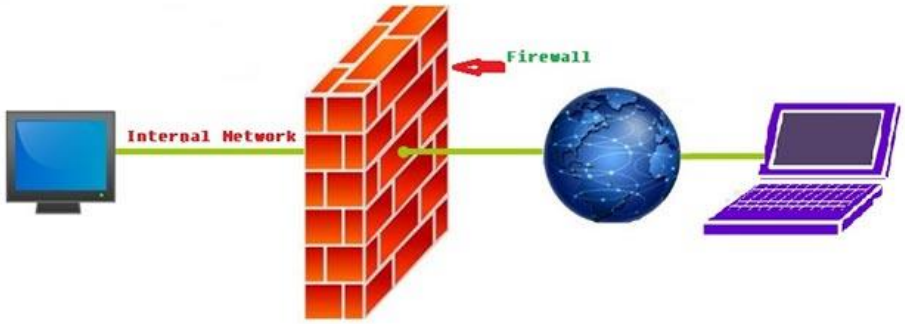
Tường lửa và IDS/IPS

Số tín chỉ: 2
Số tiết: 30 tiết
(Lý Thuyết)

GV: ThS. Nguyễn Thị Phong Dung
Email : ntpdung@ntt.edu.vn

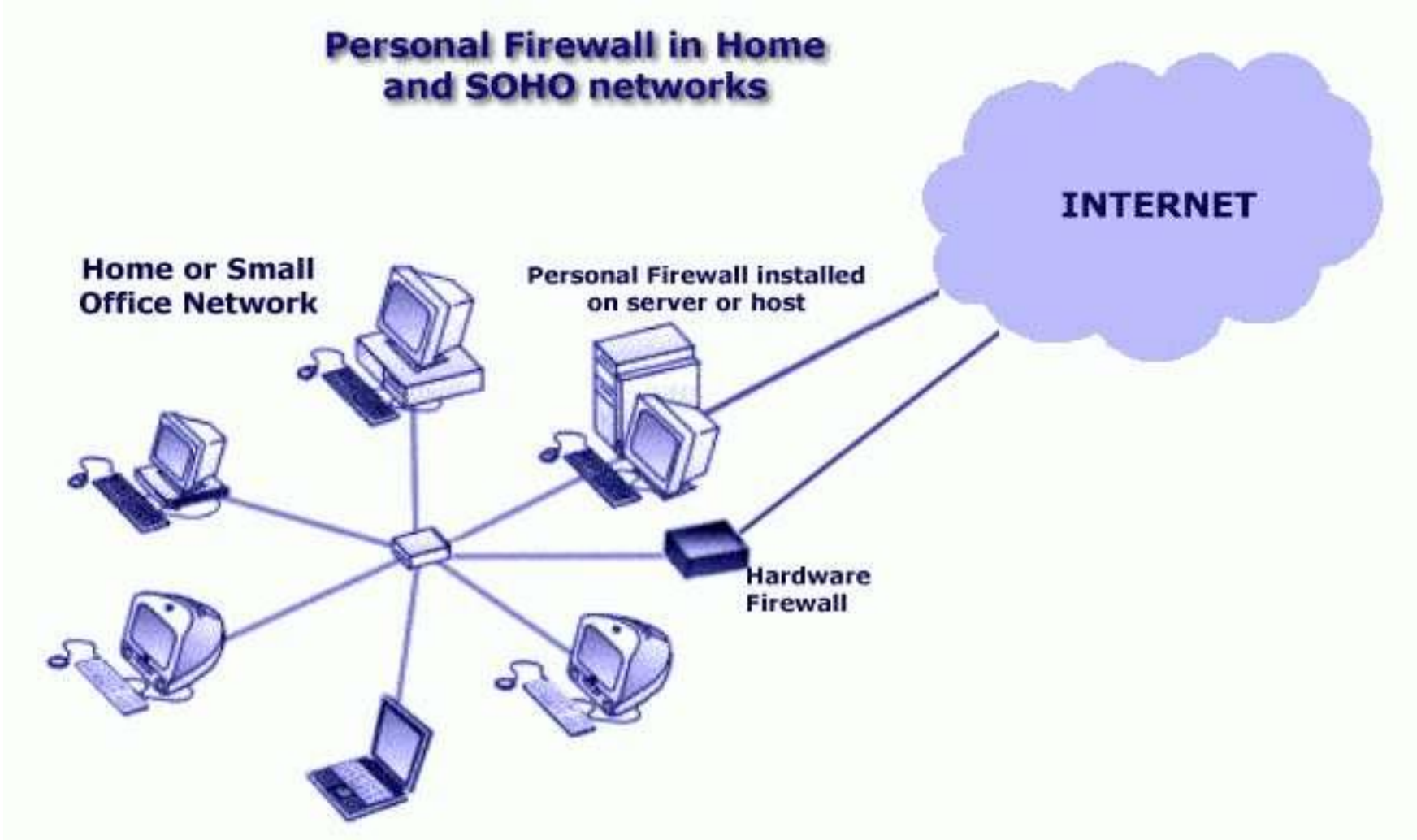
Tường lửa

- **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 – cụ thể hóa bằng các luật).
  - 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



Tường lửa

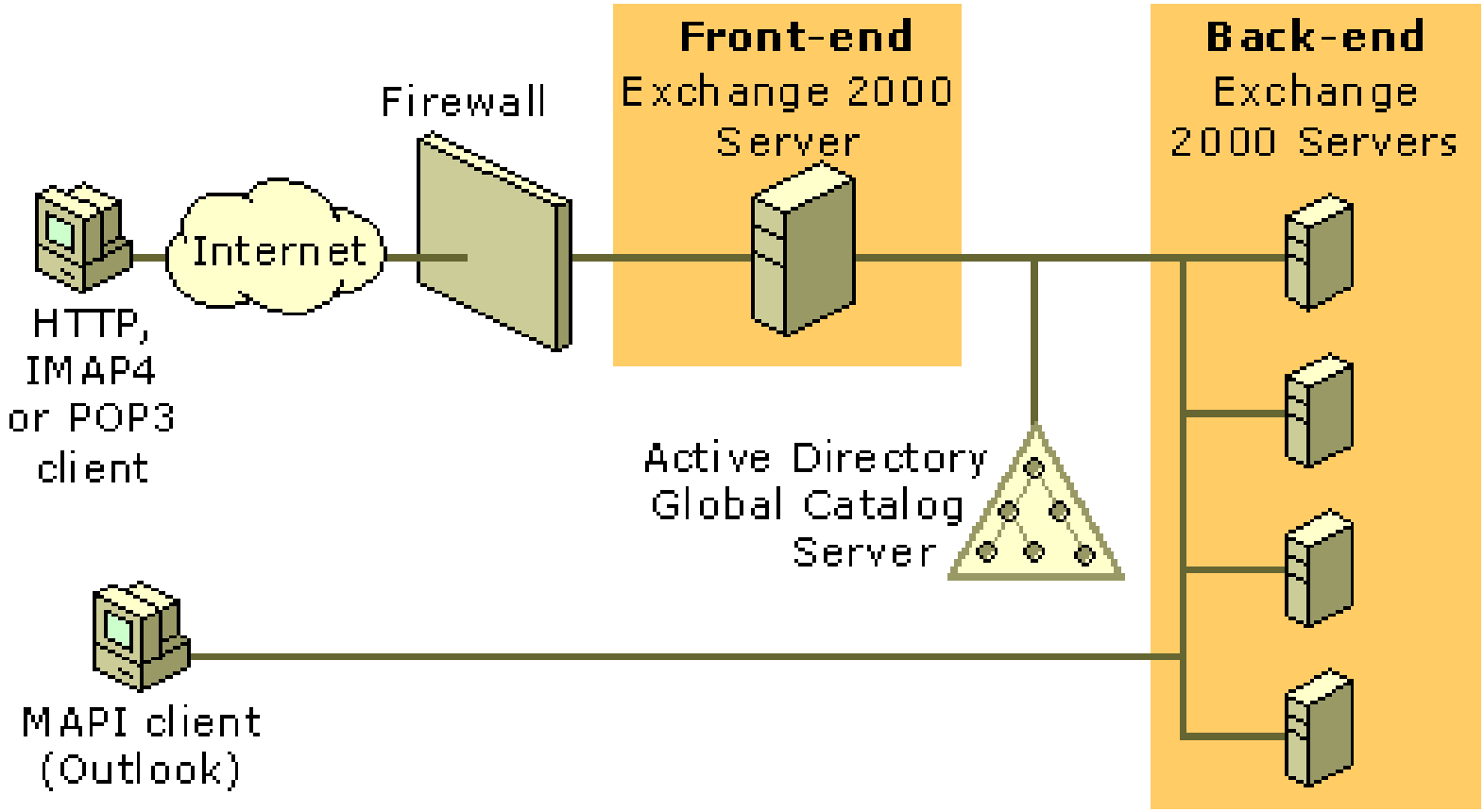
- **Topo mạng với tường lửa:**



Tường lửa

- **Topo mạng với tường lửa:**

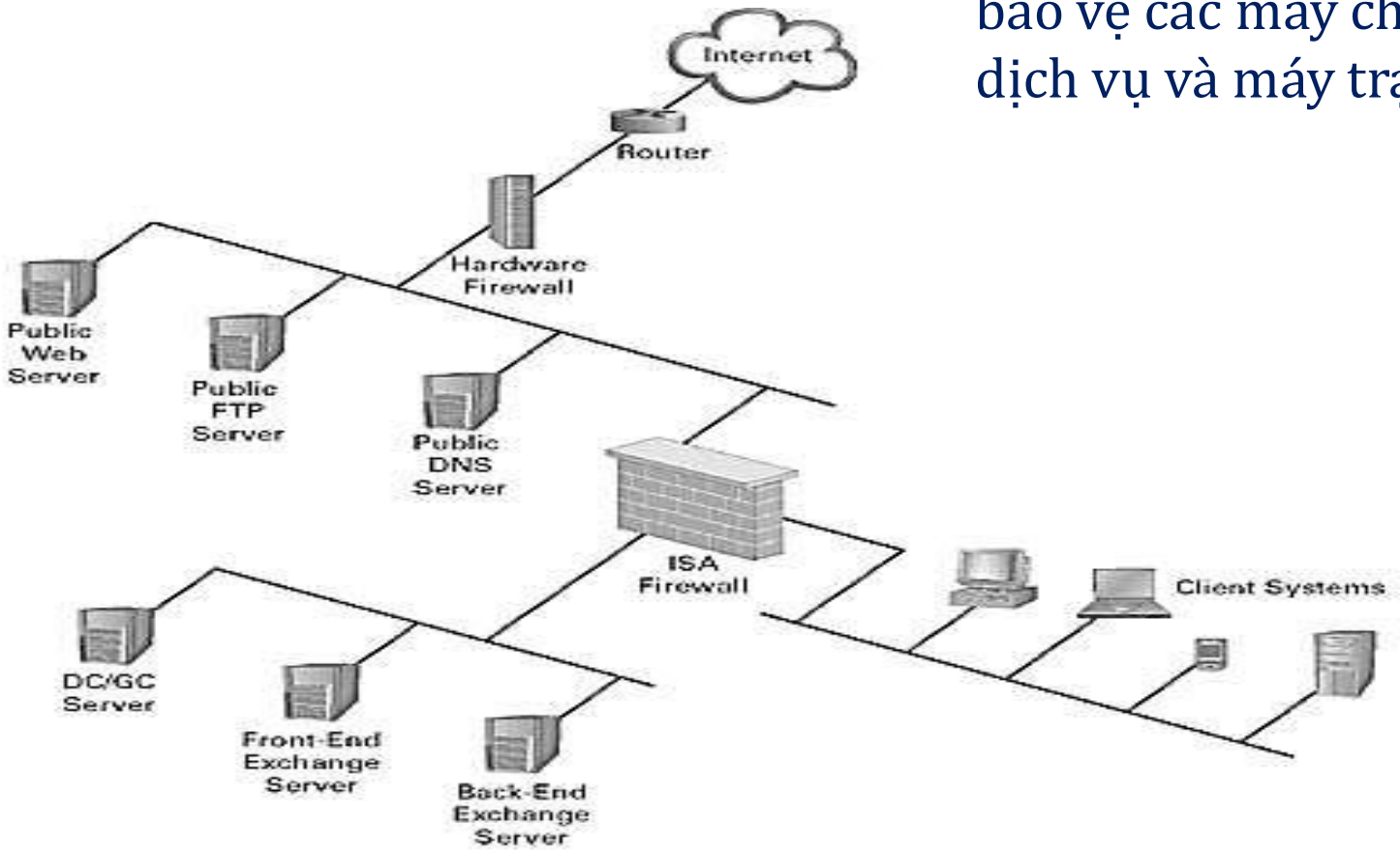
Tường lửa bảo vệ các máy chủ dịch vụ



Tường lửa

- **Topo mạng với tường lửa:**

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

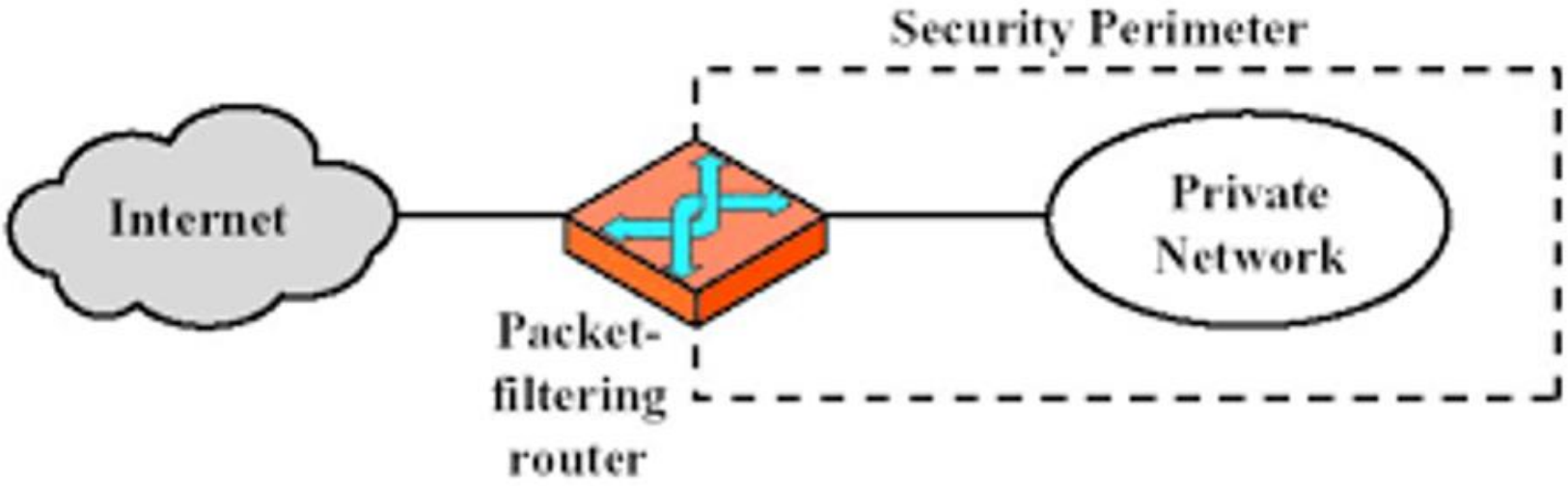


Back-to-back firewall network protecting an OWA Web site.

Tường lửa

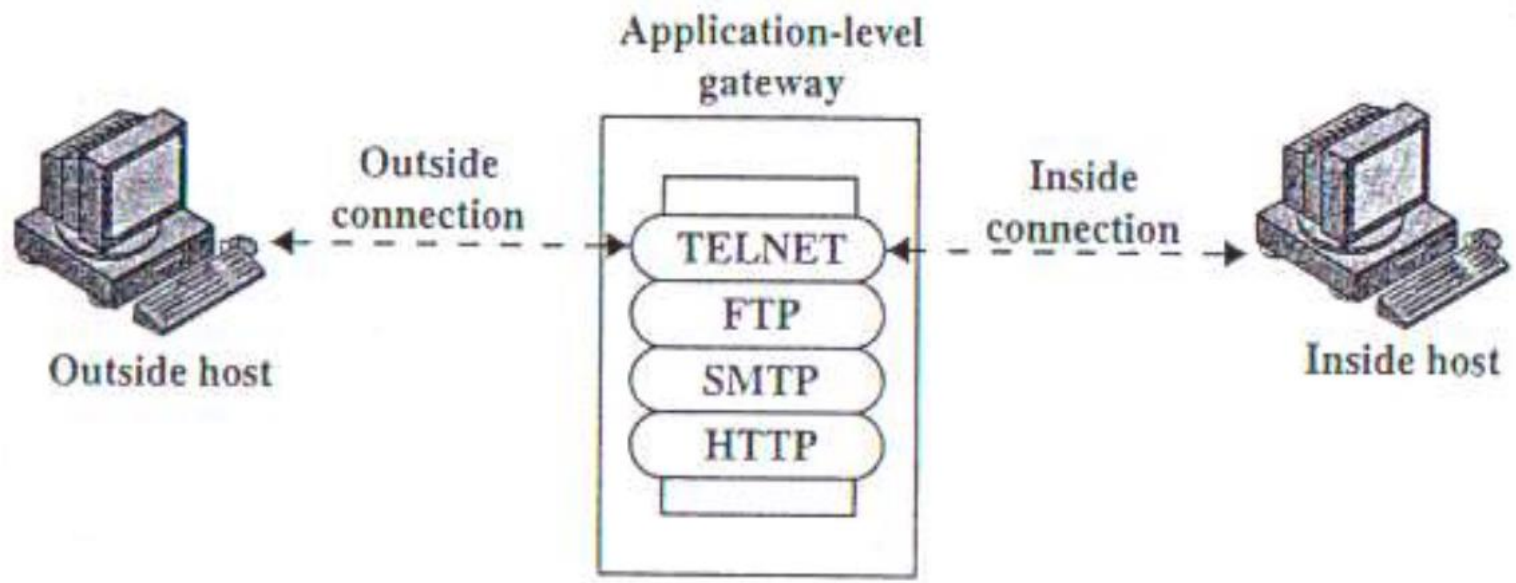
- **Các loại tường lửa:**
  - **Lọc gói tin (Packet-Filtering):**
  - Áp dụng một tập các luật cho mỗi gói tin đi/đến để quyết định chuyển tiếp hay loại bỏ gói tin.
  - Các tường lửa dạng này thường lọc gói tin lớp IP.
  - **Các cổng ứng dụng (Application-level gateway):**
  - Còn gọi là proxy server, thường dùng để phát lại (relay) traffic của mức ứng dụng.
  - Tường lửa ứng dụng web (WAF – Web Application Firewall) là dạng cổng ứng dụng được sử dụng rộng rãi.
  - **Cổng chuyển mạch (Circuit-level gateway):**
  - Hoạt động tương tự các bộ chuyển mạch.

- **Lọc gói tin (Packet Filtering):**



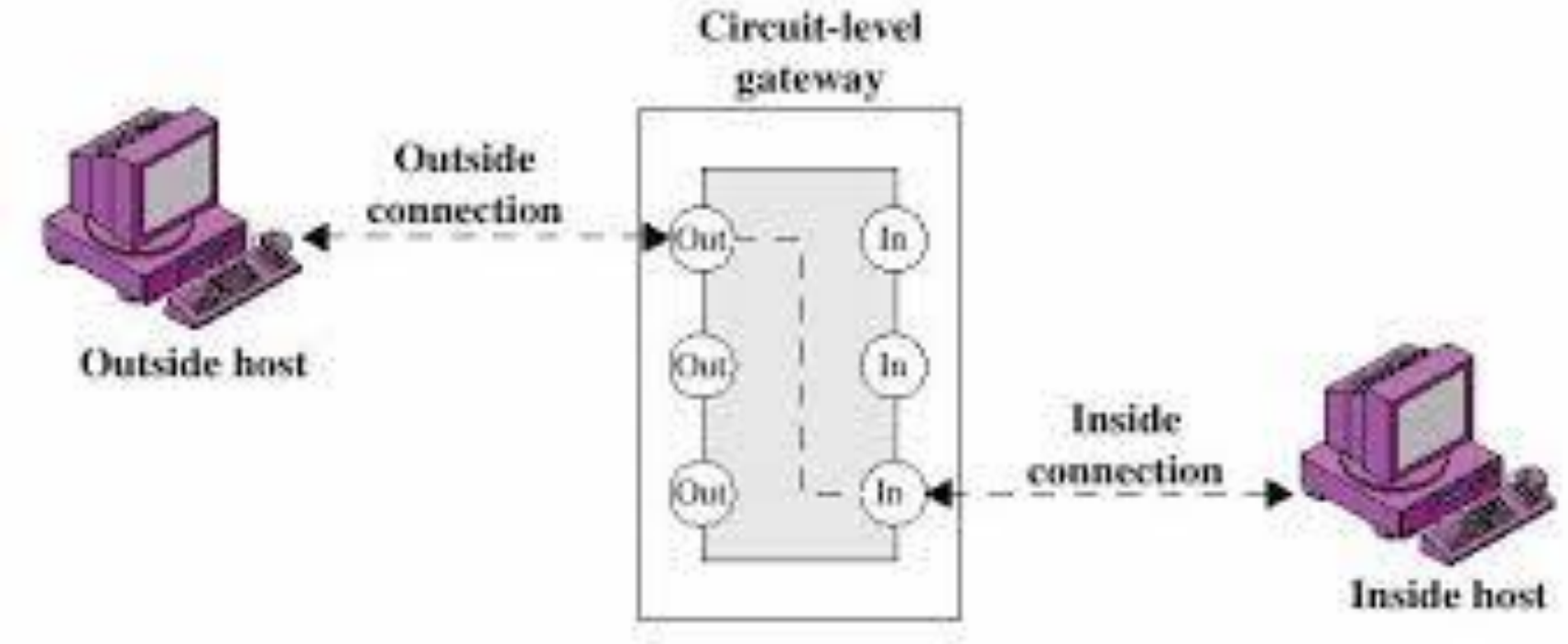
Tường lửa

- **Cổng ứng dụng (Application-level gateway):**



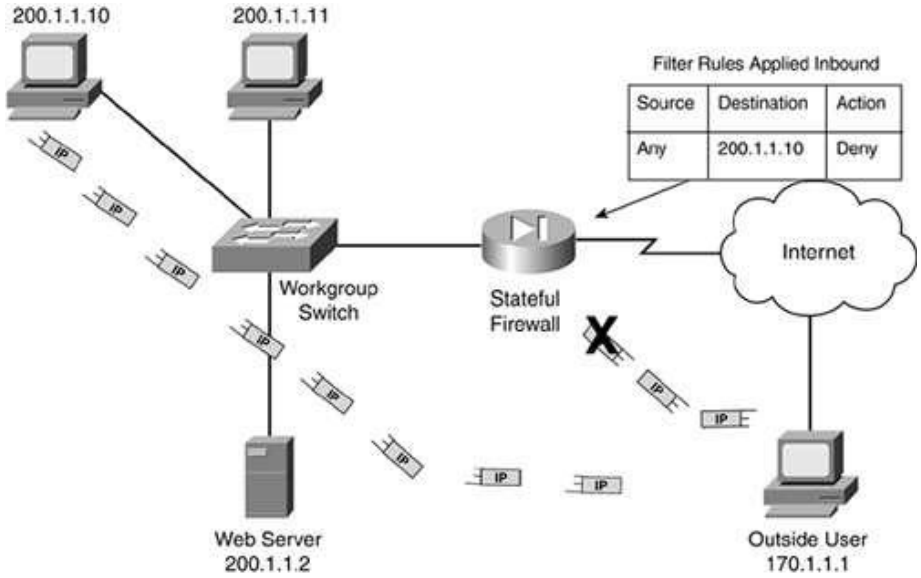
Tường lửa

- **Cổng chuyển mạch (Circuit-level gateway):**



Tường lửa

- **Lọc 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 các 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.



Tường lửa

- **Lọc 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.

Tường lửa

- **Kỹ thuật kiểm soát truy cập**
  - **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.

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.

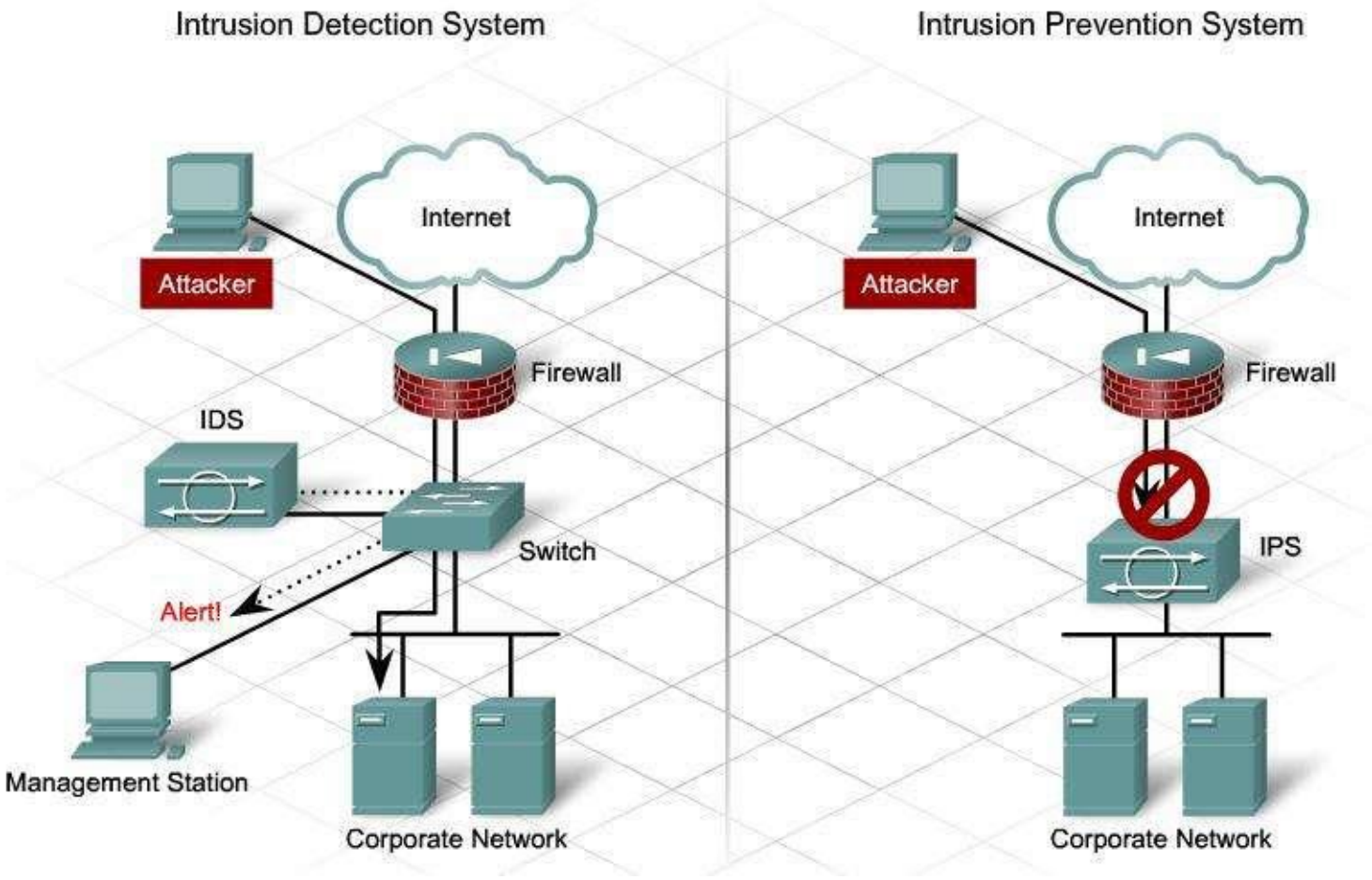
IDS/IPS

- Các hệ thống phát hiện/ngăn chặn tấn công, xâm nhập (IDS/IPS) thường được sử dụng như một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng;
- Không thể chống lại các tấn công không đi qua nó.
  - **IDS – Intrusion Detection System**:
  - Hệ thống phát hiện tấn công, xâm nhập;
  - **IPS - Intrusion Prevention System:**
  - Hệ thống ngăn chặn tấn công, xâm nhập.

Các hệ thống IDS/IPS có thể được đặt trước hoặc sau tường lửa, tùy theo mục đích sử dụng.

IDS/IPS

- **Các hệ thống ngăn chặn/phát hiện tấn công, xâm nhập**



IDS/IPS

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

- **So sánh IDS/IPS:**

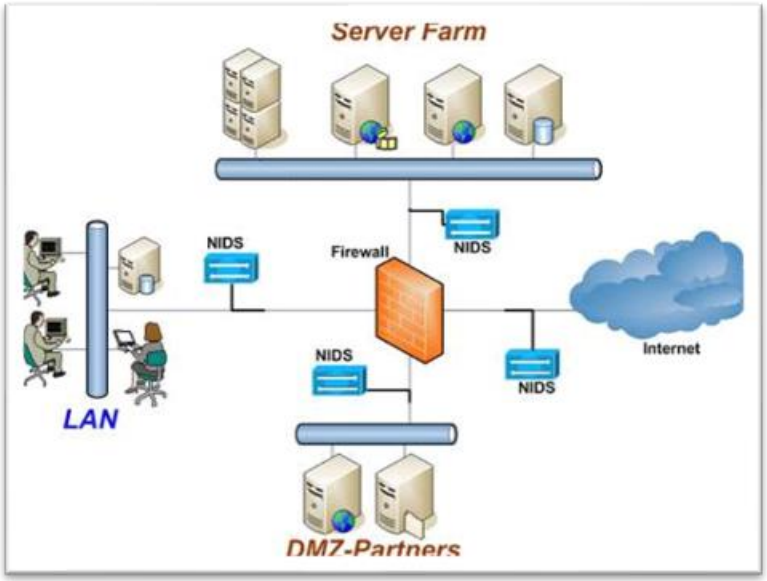
  Giống: Về cơ bản IPS và IDS giống nhau về chức năng giám sát.

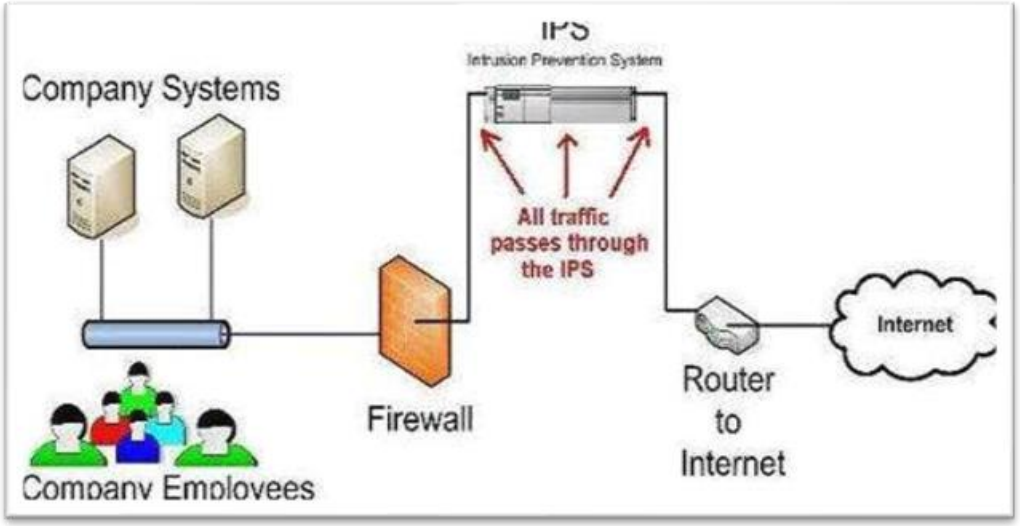
  Khác:

  • IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công/xâm 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 báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

IDS/IPS


Server Farm
NIDS
Firewall
NIDS
Internet
NIDS
NIDS
LAN
DMZ-Partners


IPS
Intrusion Prevention System
Company Systems
All traffic passes through the IPS
Internet
Router to Internet
Firewall
Company Employees

- **Phân loại:**

❑ Theo nguồn dữ liệu:

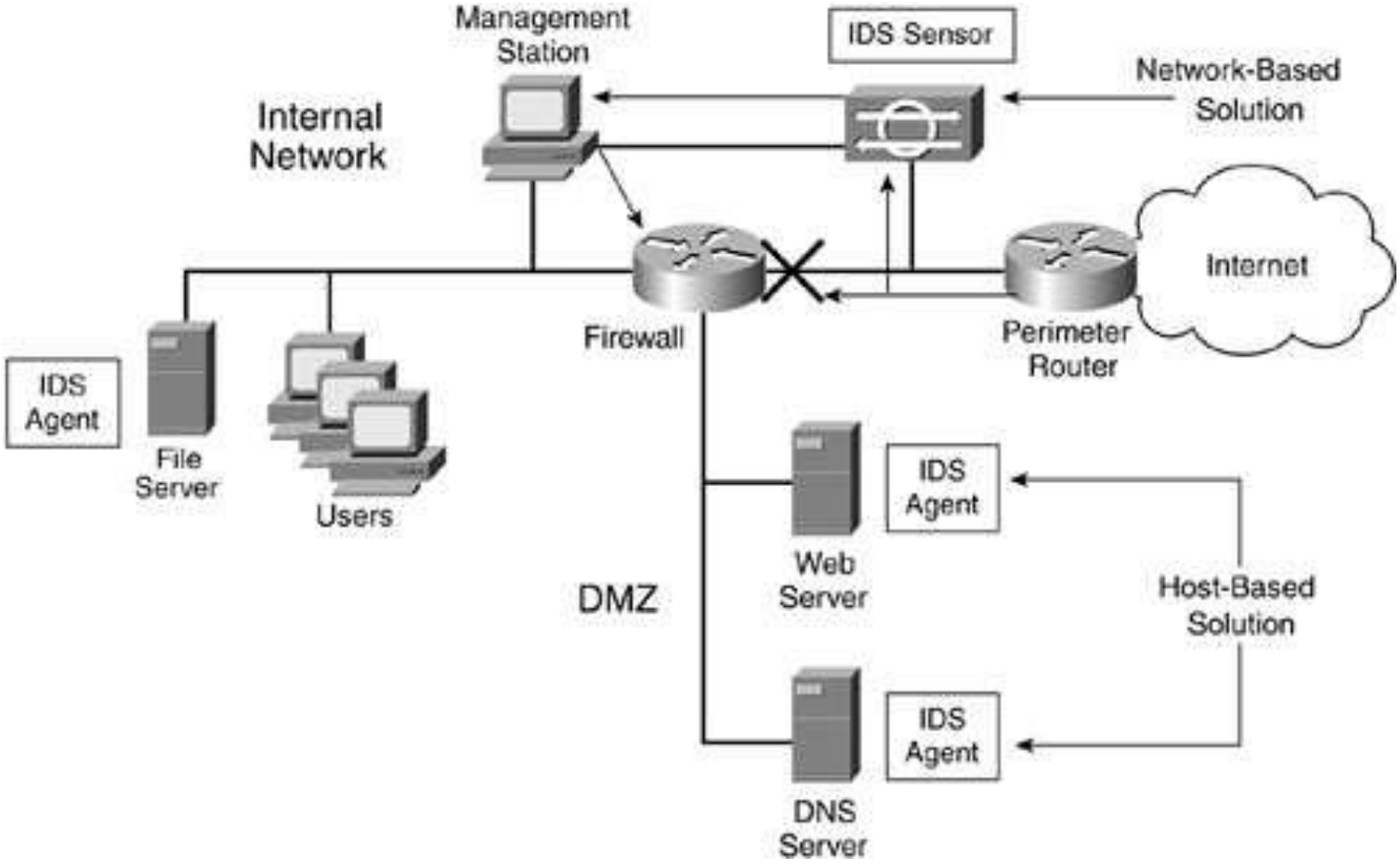
- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS): phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng.
- Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS): phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho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

- **Phân loại:**

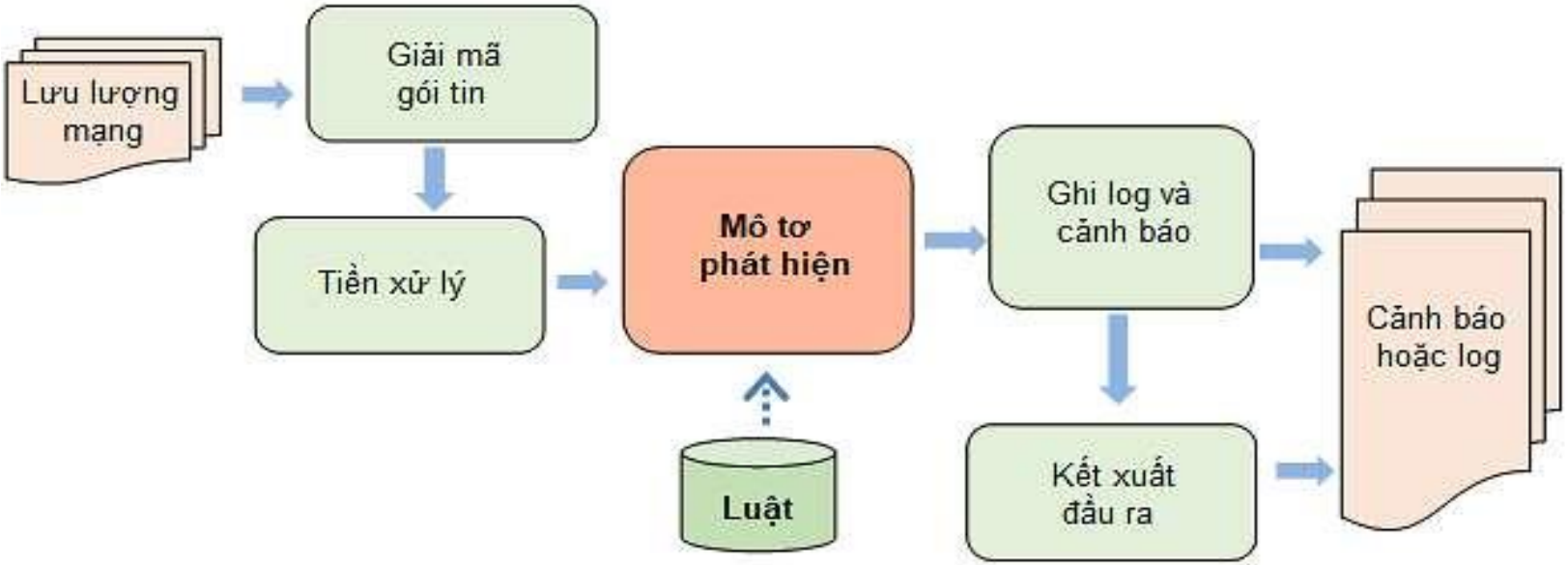
❑ **Theo kỹ thuật phân tích:**

- Phát hiện xâm nhập dựa trên chữ ký hoặc phát hiện sự lạm dụng (Signature-based / misuse instrusion detection);
- Phát hiện xâm nhập dựa trên các bất thường (Anomaly instrusion detection)

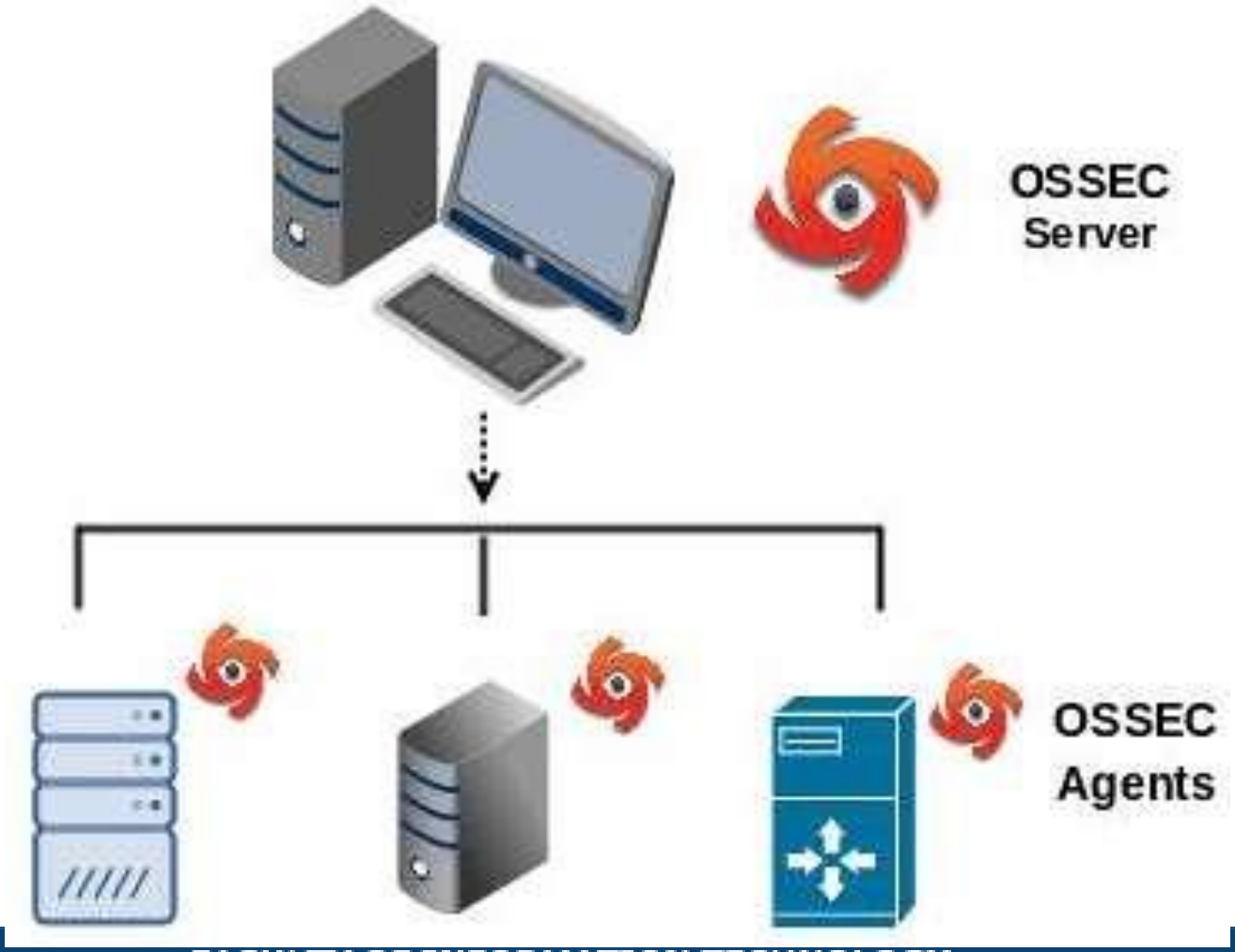
- **NIDS và HIDS**


Management Station
IDS Sensor
Network-Based Solution
Internal Network
Internet
Firewall
Perimeter Router
IDS Agent
File Server
Users
IDS Agent
Web Server
DMZ
Host-Based Solution
IDS Agent
DNS Server

- **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

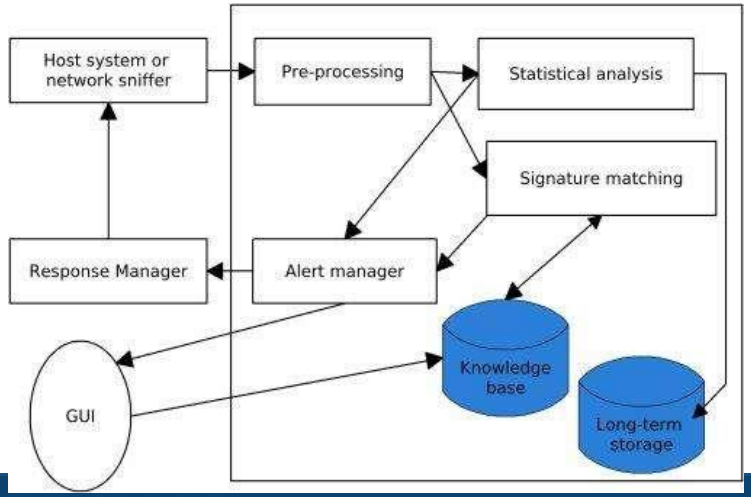
- **HIDS - OSSEC**



- **Phát hiện xâm nhập dựa trên chữ ký**

Xây dựng cơ sở dữ liệu các chữ ký/dấu hiệu của các loại tấn công, xâm 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, xâm nhập.



- **Phát hiện xâm nhập dựa trên chữ ký**

❑ **Ưu điểm:**

- Có khả năng phát hiện các tấn công, xâm 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, xâm 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

- **Phát hiện xâm nhập dựa trên bất thường**

❑ **Phương pháp này dựa trên giả thiết:**

Các hành vi xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường.

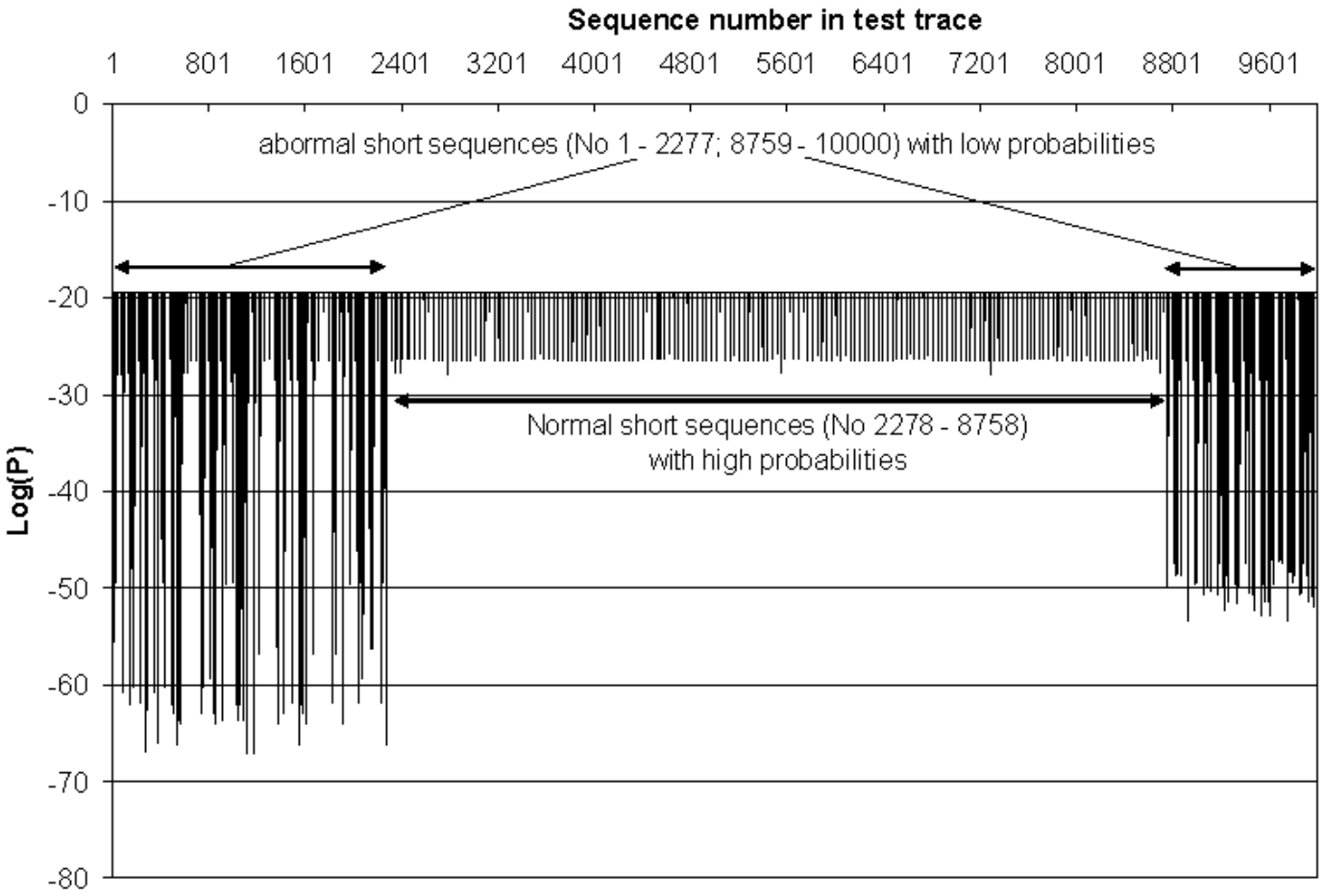
❑ **Quá trình xây dựng và triển khai gồm 2 giai đoạn:**

- 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.

- **Phát hiện xâm nhập dựa trên bất thường**

Ví dụ:

Tình trạng bình thường (Log(P) lớn) và bất thường (Log(P) rất nhỏ)

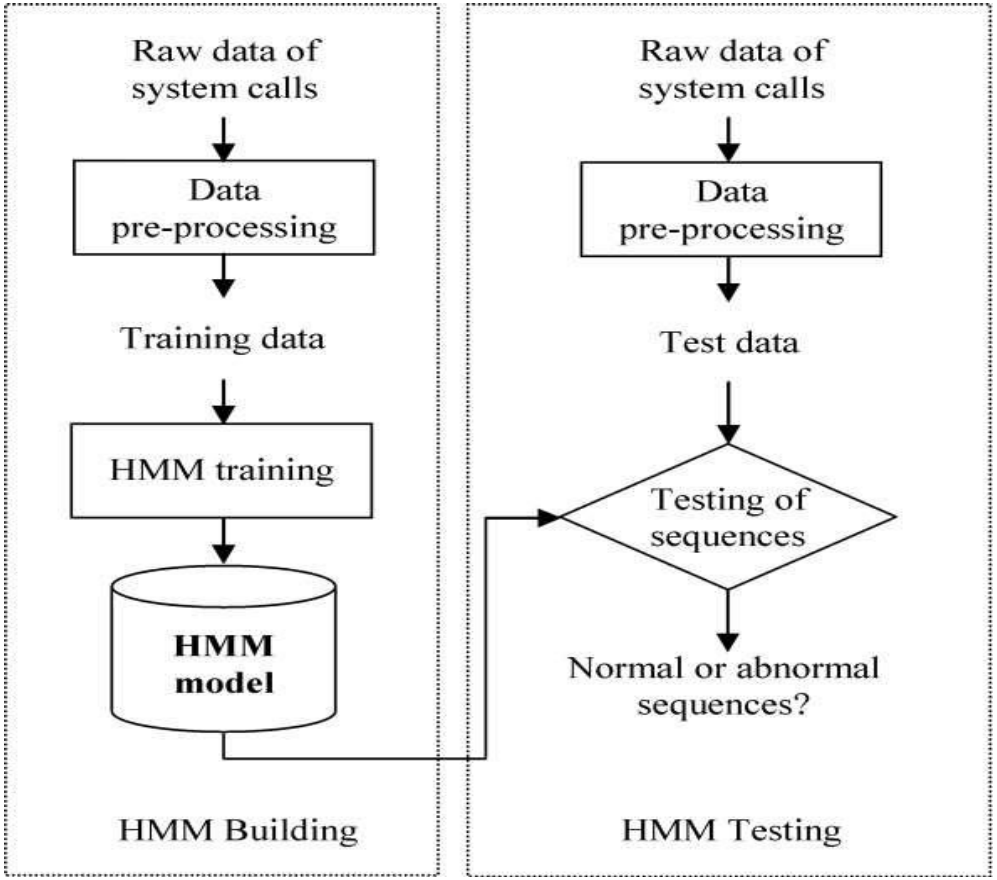


- **Phát hiện xâm nhập dựa trên bất thường**

HMM-Based

Anomaly

Detection



- **Phát hiện xâm nhập dựa trên bất thường**

❑ **Ưu điểm:**

- Có tiềm năng phát hiện các loại xâm 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

IDS/IPS

- **Phát hiện xâm nhập dựa trên bất thường**

❑ **Các phương pháp xử lý, phân tích dữ liệu và mô hình hóa trong phát hiện xâm 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).*

Cám ơn !