Chương 3.
Công nghệ phát hiện xâm nhập mạng

Nội dung bài giảng:

1. Đặt vấn đề
2. Định nghĩa IDS/IPS
3. Phân loại
4. Kỹ thuật phát hiện
5. Cấu trúc hệ thống
6. Một số sản phẩm

1. Đặt vấn đề

- Các hiểm họa trong mạng máy tính
- Điểm yếu của tường lửa
- Rủi ro mất ATTT tới dữ liệu, tài nguyên mạng

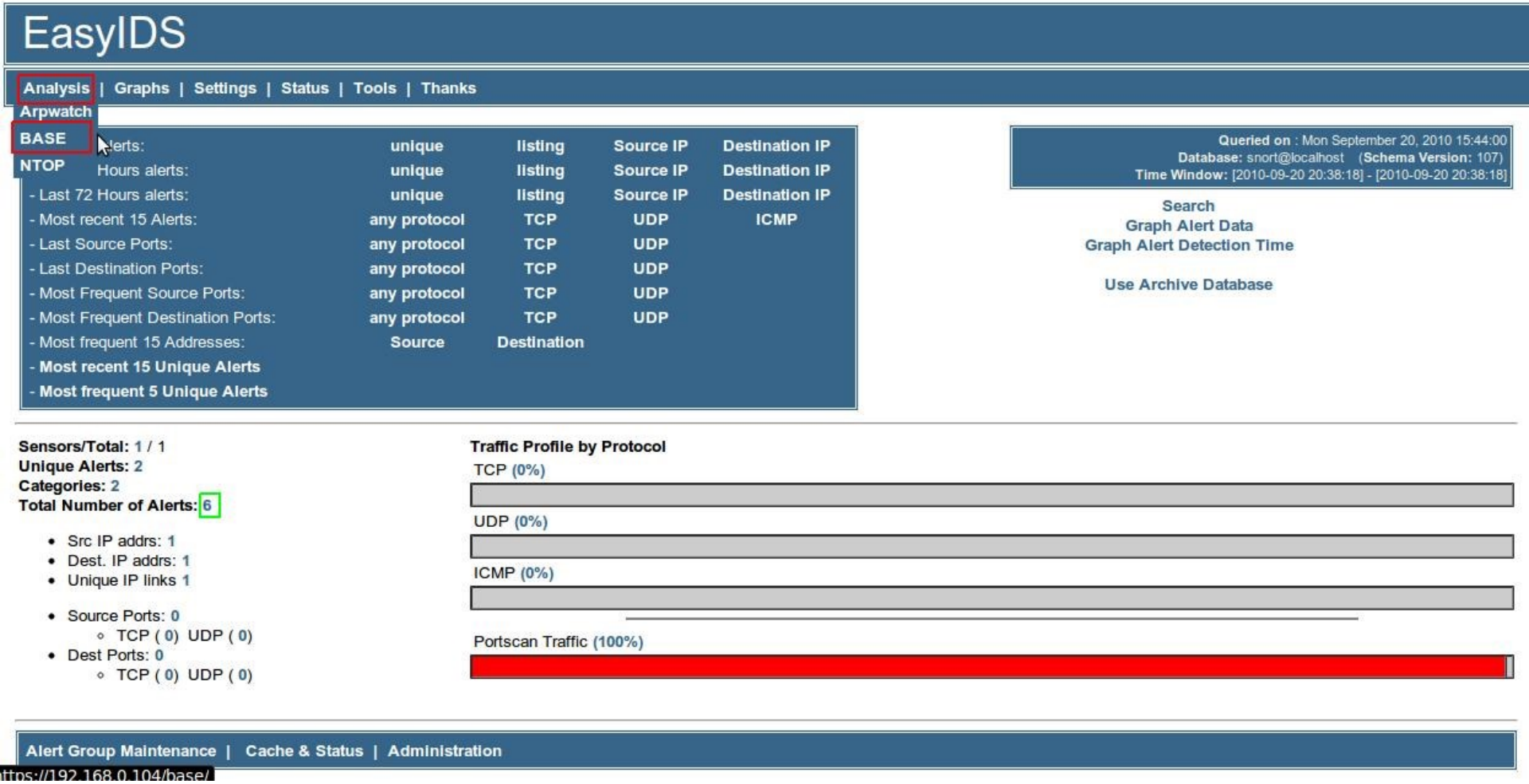
2. Định nghĩa

- IDS (Intrution Detection System): là 1 thiết bị hoặc phần mềm chịu trách nhiệm theo dõi hệ thống mạng để kịp thời phát hiện ra những hoạt động bất thường hoặc những vi phạm chính sách gây hại cho hệ thống và thông báo cho người quản trị.
- IPS (Intrution Prevention System): hoạt động tương tự như IDS nhưng có thêm chức năng ngăn chặn tấn công.

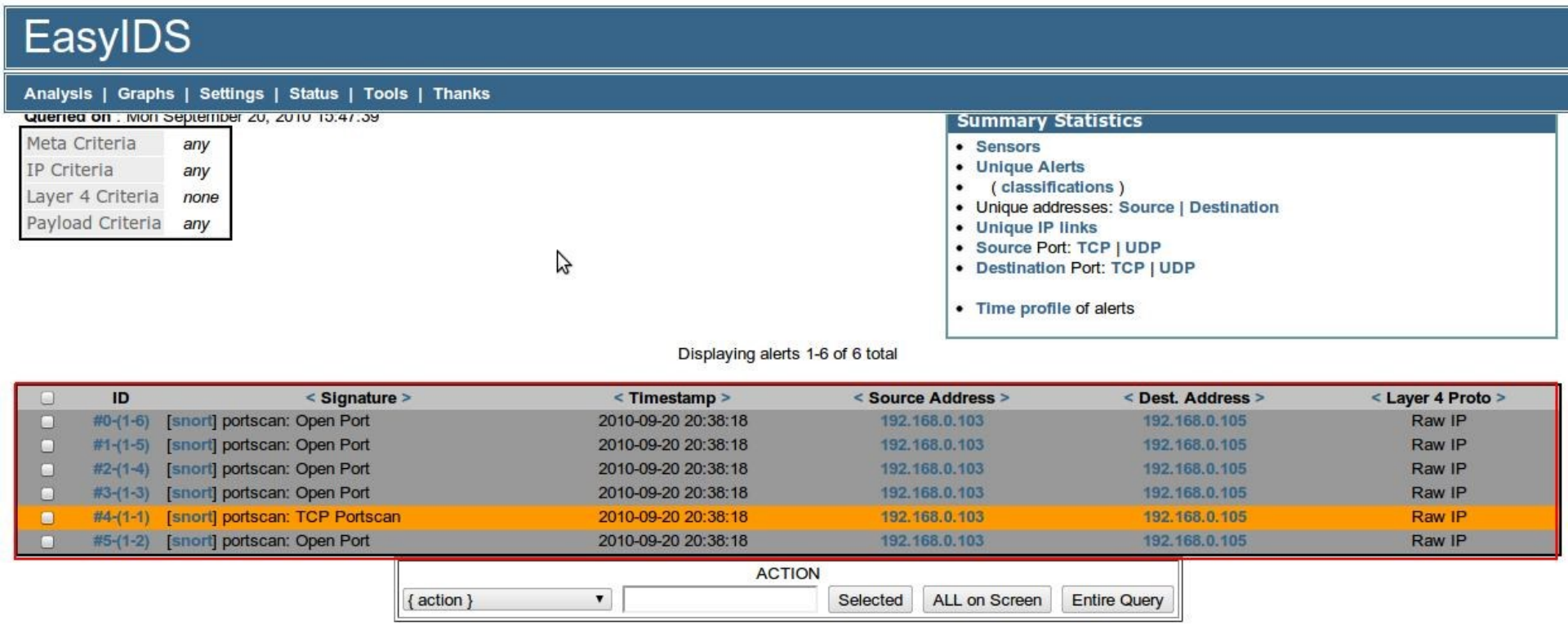
2. Chức năng

- Theo dõi các hoạt động bất thường đối với hệ thống.
- Xác định ai đang tác động đến hệ thống và cách thức như thế nào.
- Các hoạt động xâm nhập xảy ra tại vị trí nào trong cấu trúc mạng.
- Cảnh báo.
- Ngăn chặn tấn công.
- Ghi log

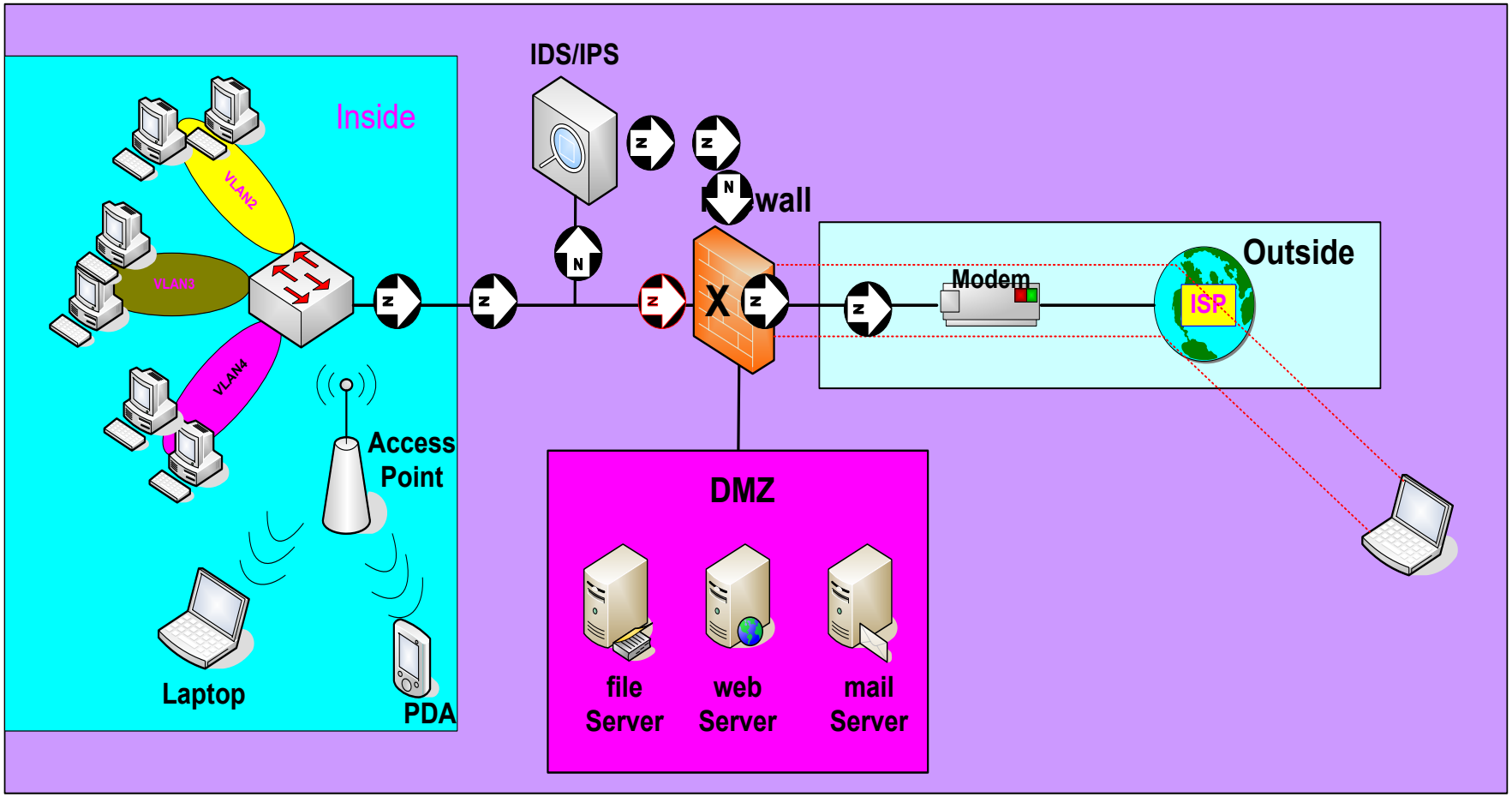
2. Chức năng


EasyIDS
Analysis | Graphs | Settings | Status | Tools | Thanks
Arpwatch
BASE
NTOP
Alerts: unique listing Source IP Destination IP
Hours alerts: unique listing Source IP Destination IP
- Last 72 Hours alerts: unique listing Source IP Destination IP
- Most recent 15 Alerts: any protocol TCP UDP ICMP
- Last Source Ports: any protocol TCP UDP
- Last Destination Ports: any protocol TCP UDP
- Most Frequent Source Ports: any protocol TCP UDP
- Most Frequent Destination Ports: any protocol TCP UDP
- Most frequent 15 Addresses: Source Destination
- Most recent 15 Unique Alerts
- Most frequent 5 Unique Alerts
Queried on : Mon September 20, 2010 15:44:00
Database: snort@localhost (Schema Version: 107)
Time Window: [2010-09-20 20:38:18] - [2010-09-20 20:38:18]
Search
Graph Alert Data
Graph Alert Detection Time
Use Archive Database
Sensors/Total: 1 / 1
Unique Alerts: 2
Categories: 2
Total Number of Alerts: 6
Src IP addrs: 1
Dest. IP addrs: 1
Unique IP links 1
Source Ports: 0
TCP (0) UDP (0)
Dest Ports: 0
TCP (0) UDP (0)
Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (100%)
Alert Group Maintenance | Cache & Status | Administration
https://192.168.0.104/base/

2. Chức năng


EasyIDS
Analysis | Graphs | Settings | Status | Tools | Thanks
Queried on : Mon September 20, 2010 15:47:39
Meta Criteria any
IP Criteria any
Layer 4 Criteria none
Payload Criteria any
Summary Statistics
Sensors
Unique Alerts
(classifications)
Unique addresses: Source | Destination
Unique IP links
Source Port: TCP | UDP
Destination Port: TCP | UDP
Time profile of alerts
Displaying alerts 1-6 of 6 total
ID < Signature > < Timestamp > < Source Address > < Dest. Address > < Layer 4 Proto >
#0-(1-6) [snort] portscan: Open Port 2010-09-20 20:38:18 192.168.0.103 192.168.0.105 Raw IP
#1-(1-5) [snort] portscan: Open Port 2010-09-20 20:38:18 192.168.0.103 192.168.0.105 Raw IP
#2-(1-4) [snort] portscan: Open Port 2010-09-20 20:38:18 192.168.0.103 192.168.0.105 Raw IP
#3-(1-3) [snort] portscan: Open Port 2010-09-20 20:38:18 192.168.0.103 192.168.0.105 Raw IP
#4-(1-1) [snort] portscan: TCP Portscan 2010-09-20 20:38:18 192.168.0.103 192.168.0.105 Raw IP
#5-(1-2) [snort] portscan: Open Port 2010-09-20 20:38:18 192.168.0.103 192.168.0.105 Raw IP
ACTION
{ action }
Selected
ALL on Screen
Entire Query

3. Mô hình triển khai



4. Phân loại

- **Network based**

  Phát hiện xâm nhập trên toàn mạng

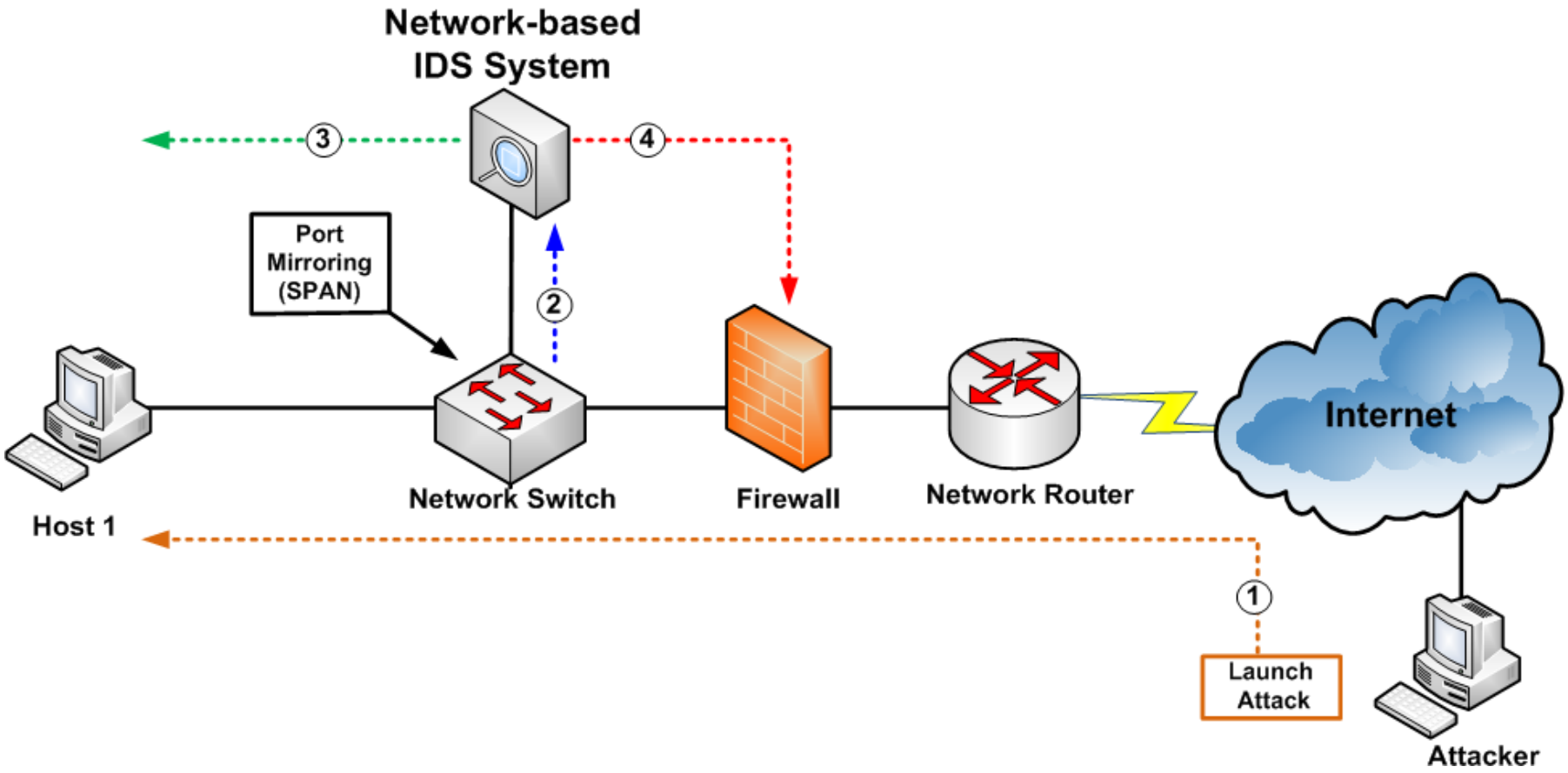
- **Host based**

  Phát hiện xâm nhập trên các máy

- **Wireless IDPS**

  Phát hiện xâm nhập cho mạng không dây

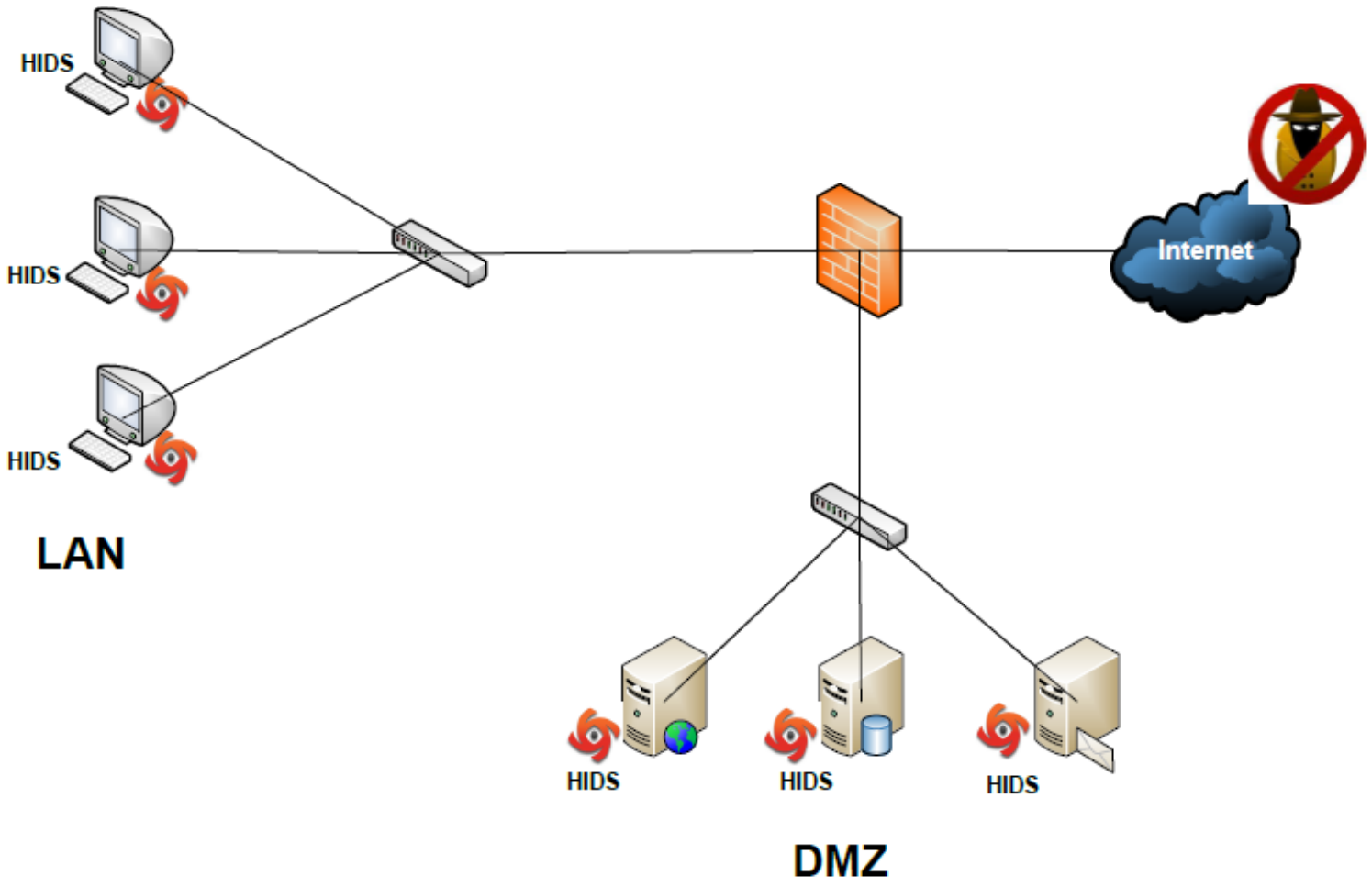
Network based IDS



Network based IDS

- Thường dưới dạng thiết bị chuyên dụng.
- Theo dõi được cả một phân vùng mạng (gồm nhiều host).
- Trong suốt với người sử dụng lẫn kẻ tấn công.
- Dễ cài đặt và bảo trì.
- Độc lập với OS.
- Thường xảy ra cảnh báo giả.
- Không phân tích đc lưu lượng đã được mã hóa.
- Ảnh hưởng tới chất lượng của mạng.

Host based IDS



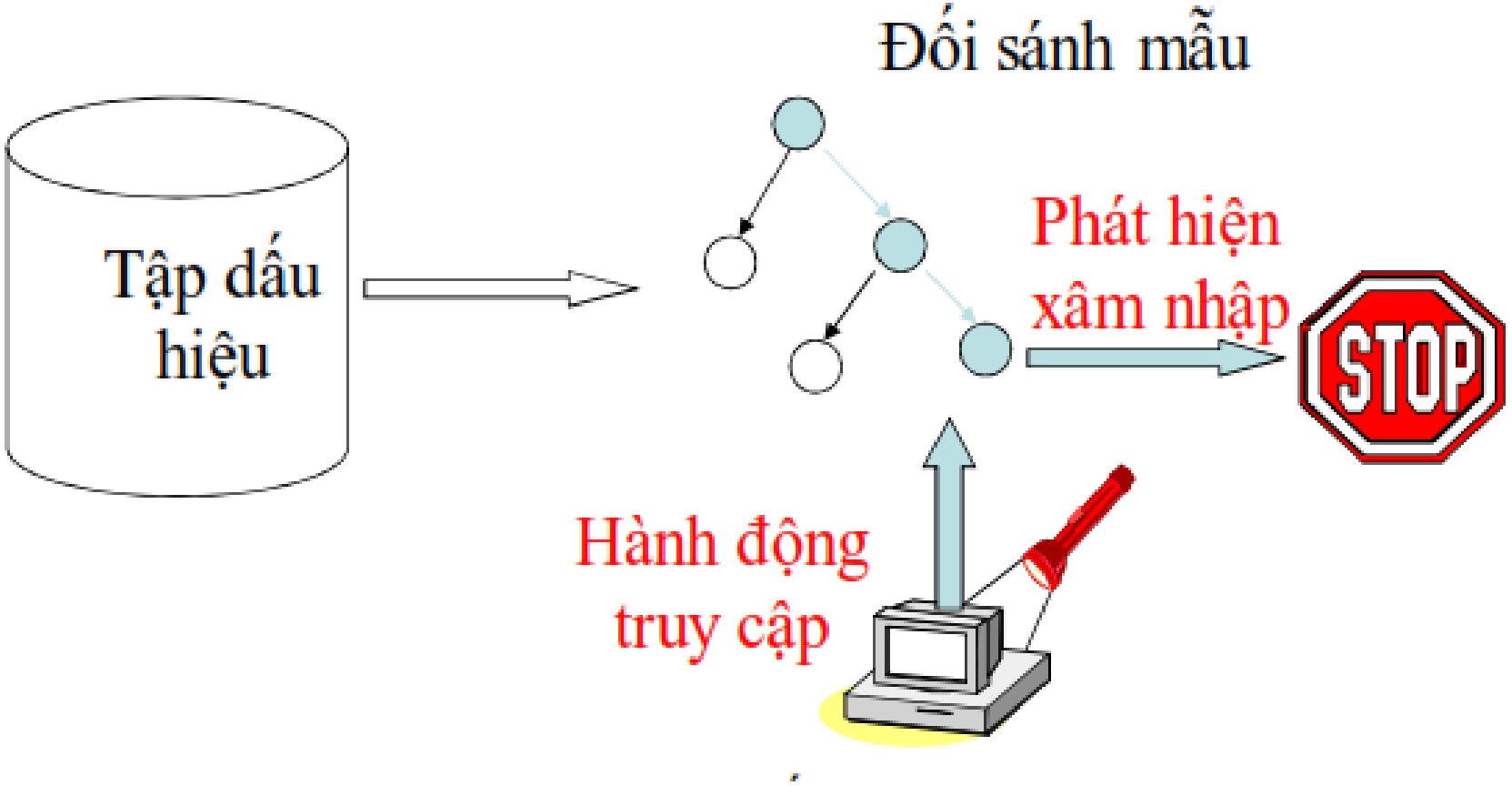
Host based IDS

- Thường dưới dạng phần mềm cài đặt.
- Có khả năng xác định người dùng liên quan tới một sự kiện.
- Có thể phân tích các dữ liệu mã hoá.
- Host IDS hoạt động phụ thuộc vào Host.
- Không có khả năng phát hiện tấn công dò quét mạng.

4. Kỹ thuật phát hiện

- Phát hiện dựa vào dấu hiệu
- Phát hiện dựa vào sự bất thường

4.1. Phát hiện dựa vào dấu hiệu



4.1. Phát hiện dựa vào dấu hiệu

- Dấu hiệu là tập hợp các mẫu hoặc nhóm thông tin cần thiết để mô tả các kiểu tấn công đã biết, thông tin này được lưu trong tập luật của hệ thống IDPS.
- Hệ thống thực hiện giám sát lưu lượng mạng và so sánh với mẫu thông tin có trong tập luật, nếu không trùng với dấu hiệu tấn công thì cho đi qua, ngược lại hệ thống thực hiện cảnh báo, ngăn chặn tấn công.
- Kỹ thuật này hiệu quả trong việc phát hiện các đe dọa đã biết, nhưng không hiệu quả trong việc phát hiện những nguy cơ chưa biết.

4.1. Phát hiện dựa vào dấu hiệu

Mẫu phát hiện tấn công DoS:

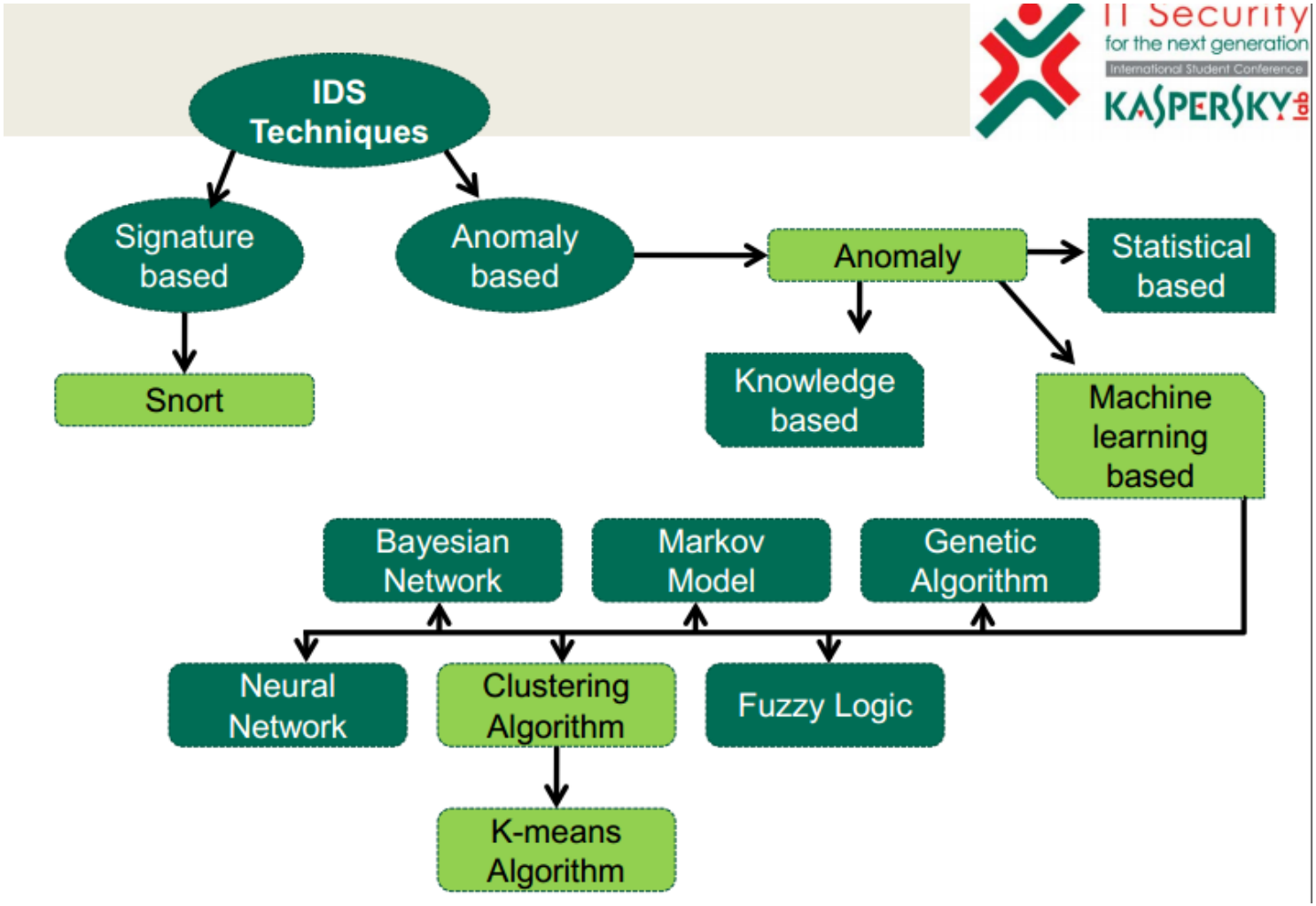
```
alert icmp any any -> any any (msg:"ICMP Ping of Death"; itype:8;
dsize:>1000; detection_filter:track by_src, count 1000, seconds 10;
sid:2100222;)
```

```
05/20/2019-09:35:48.441665  [**] [1:2100222:2] ICMP Ping of Death [**] [Classific
ation: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.139.
129:8 -> 192.168.139.138:0
05/20/2019-09:35:48.722608  [**] [1:2100222:2] ICMP Ping of Death [**] [Classific
ation: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.139.
129:8 -> 192.168.139.138:0
05/20/2019-09:35:49.284173  [**] [1:2100222:2] ICMP Ping of Death [**] [Classific
ation: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.139.
129:8 -> 192.168.139.138:0
05/20/2019-09:35:49.454991  [**] [1:2100222:2] ICMP Ping of Death [**] [Classific
ation: Detection of a Denial of Service Attack] [Priority: 2] {ICMP} 192.168.139.
129:8 -> 192.168.139.138:0
```

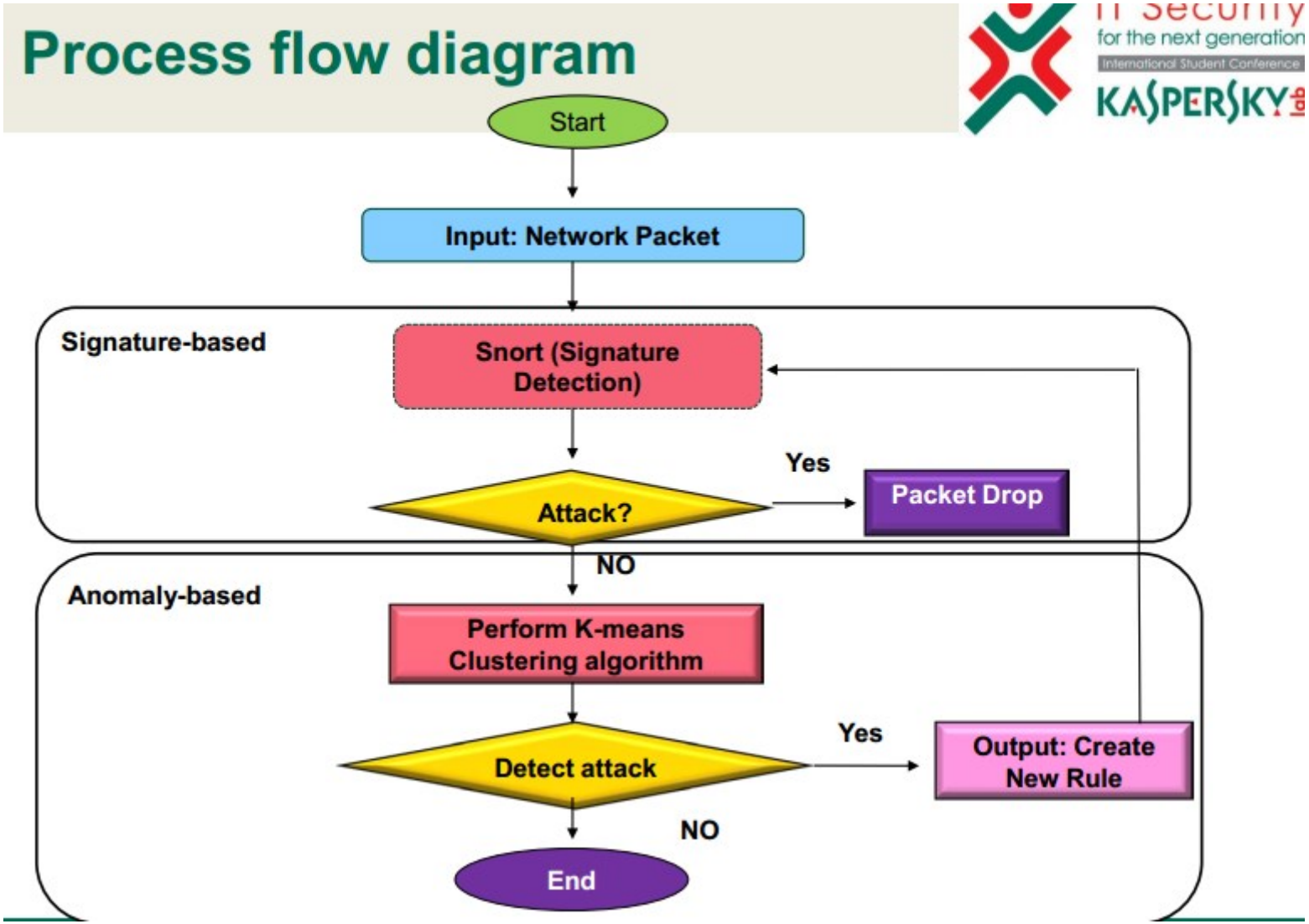
4.2. Phát hiện dựa vào sự bất thường

- Là quá trình so sánh hành động được coi là bình thường với các sự kiện đang diễn ra để xác định độ chênh lệch dẫn tới sự bất thường.
- IDS dựa vào thông tin miêu tả hành động bình thường của nhiều đối tượng như người dùng, máy chủ, các kết nối mạng, hay ứng dụng.
- Thông tin này được tạo ra bằng cách giám sát các hành động thông thường trong một khoảng thời gian để đưa ra đặc điểm nổi bật của hành động đó.
- Yêu cầu thời gian đủ lâu để học tất cả các hành động bình thường của hệ thống. (Kỹ thuật học máy – Machine Learning)

4.2. Phát hiện dựa vào sự bất thường



4.2. Phát hiện dựa vào sự bất thường



5. Thành phần của IDS/IPS

Thành phần hệ thống:

- Sensor or Agent
- Management Server
- Database Server
- Console

5. Cấu trúc IDS/IPS

Sensor or Agent:

- Là thành phần thu thập sự kiện tin từ mạng và host
- Gửi tới máy chủ quản lý tập trung

5. Cấu trúc IDS/IPS

Management Server:

- Là thành phần quản lý tập trung
- Nhận sự kiện từ bộ cảm biến
- Phân tích và phát hiện tấn công

5. Cấu trúc IDS/IPS

Database Server:

- Là thành phần lưu trữ thông tin sự kiện
- Từ bộ cảm biến và máy chủ quản lý

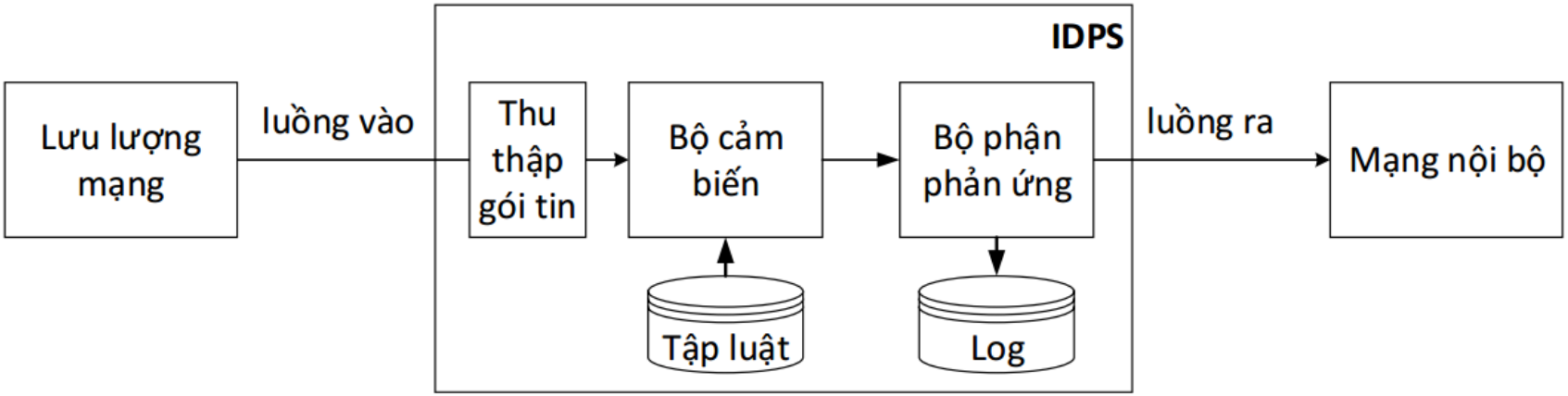
5. Cấu trúc IDS/IPS

Console:

- Là chương trình cung cấp giao diện quản trị cho người dùng
- Thông qua giao diện web hoặc dashboard

5. Cấu trúc IDS/IPS

Cấu trúc bên trong của Snort:



6. Một số sản phẩm