Chương 5 : HỆ THỐNG PHÁT HIỆN VÀ PHÒNG CHỐNG XÂM NHẬP

GV : Th.S.Nguyễn Duy

duyn@uit.edu.vn

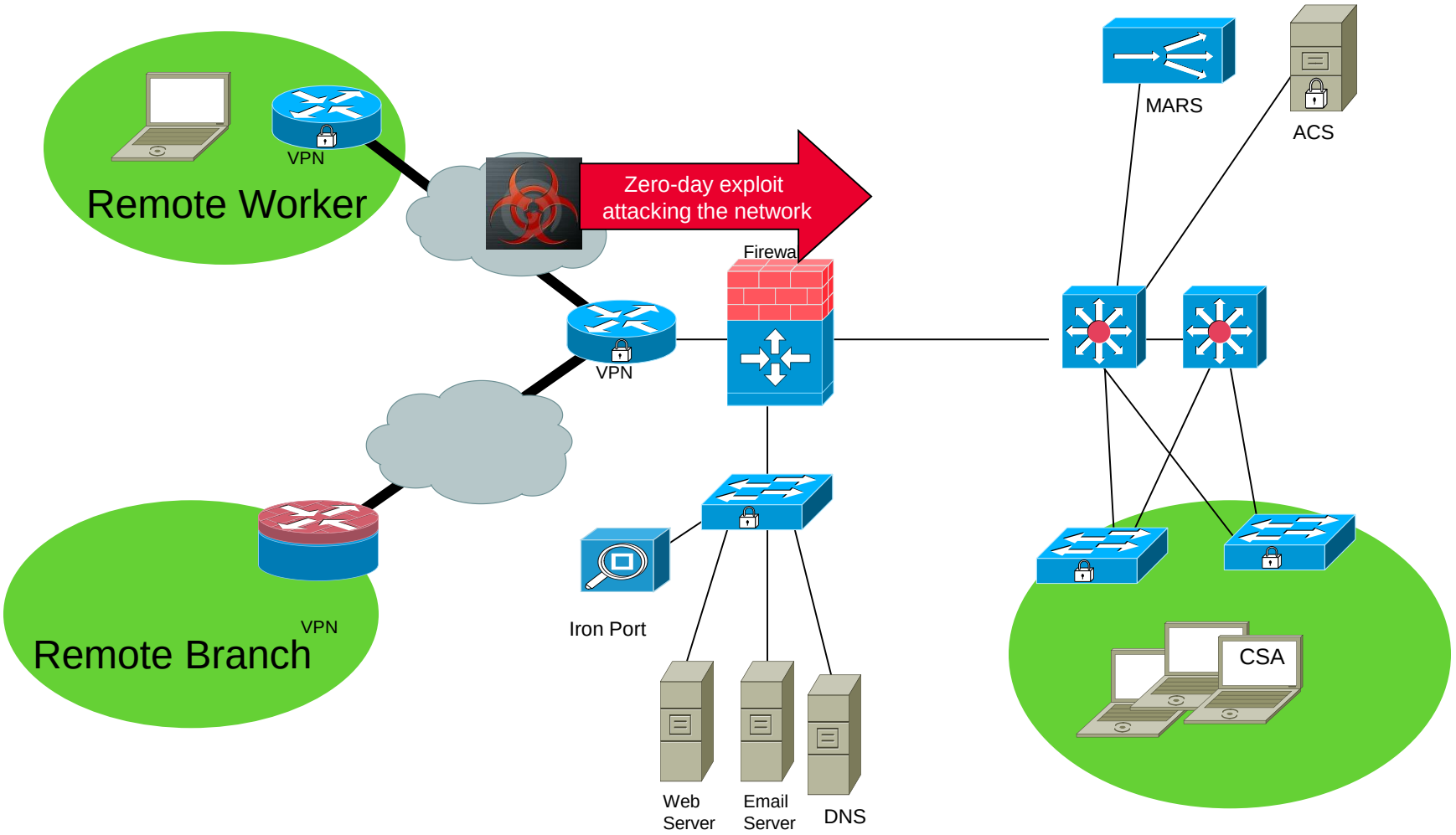
Nội dung

1. Tổng quan về IDS/IPS?
2. Thành phần chính của IDS/IPS?
3. Phân loại IDS/IPS ?
4. Các kỹ thuật phát hiện xâm nhập
5. Snort

1 Tổng quan về IDS/IPS

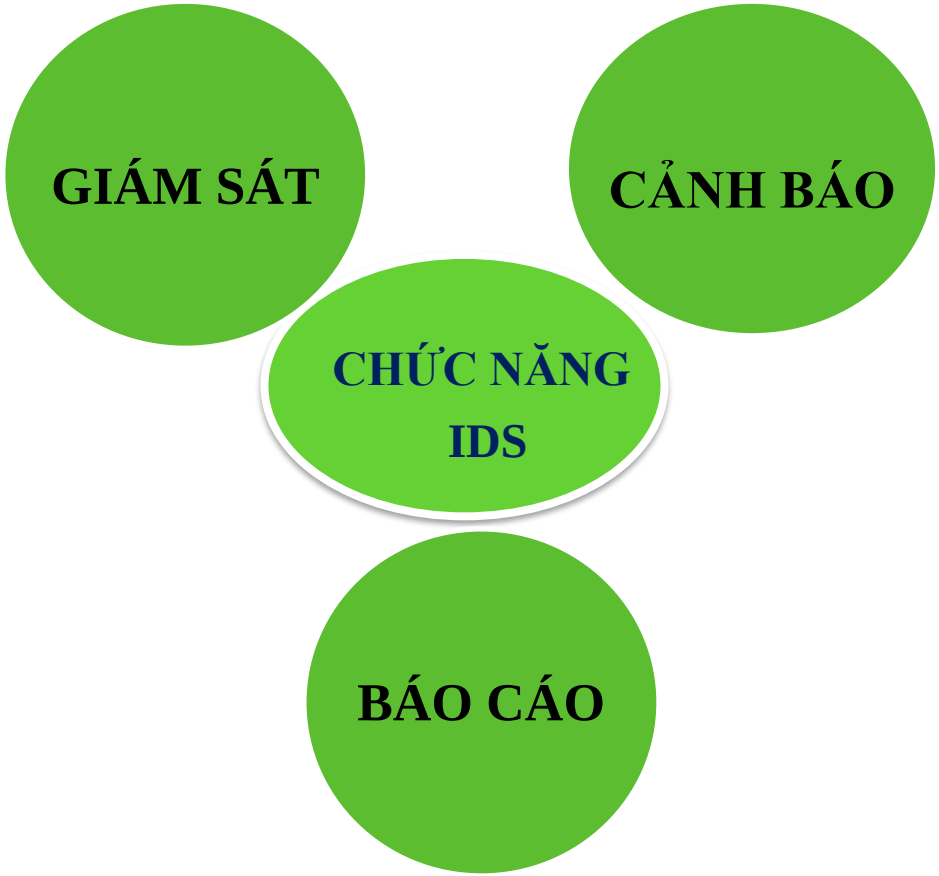
- **Intrusion Detection:** qui trình theo dõi các sự kiện xuất hiện trong hệ thống máy tính và mạng. Sau đó phân tích chúng có dấu hiệu của sự xâm nhập hay không?
- **Tại sao lại cần Intrustion Detection?**

Common Intrusions

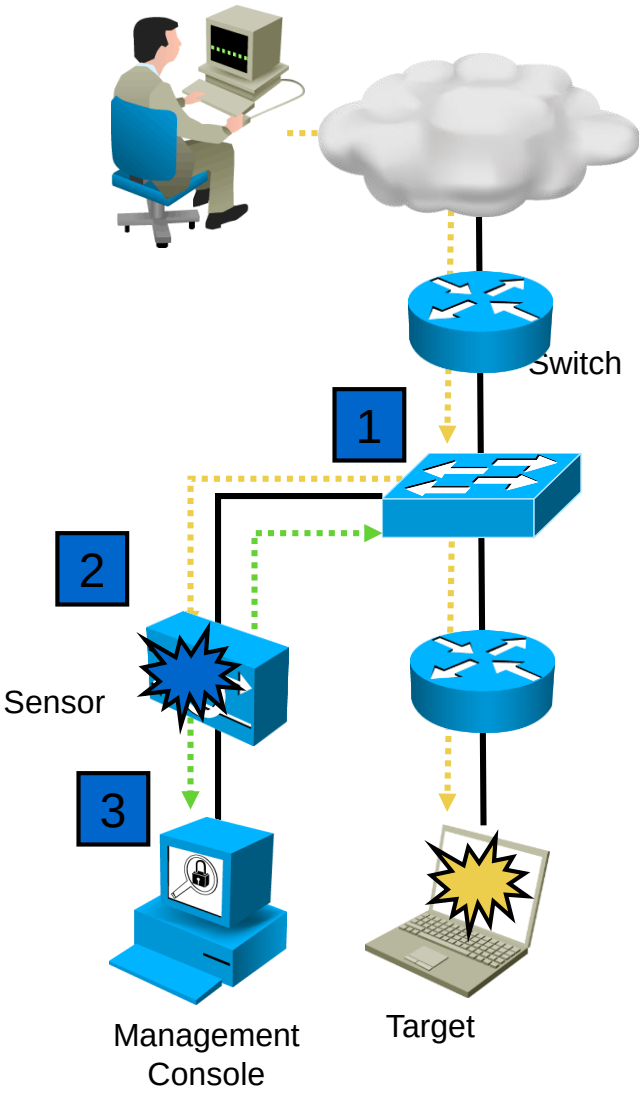


1 Tổng quan về IDS/IPS

- **Intrusion Detection System:** là một hệ thống tự động giám sát hoạt động trên hệ thống mạng và phân tích để tìm ra các dấu hiệu vi phạm đến các quy định bảo mật máy tính,chính sách sử dụng và các tiêu chuẩn an toàn thông tin.



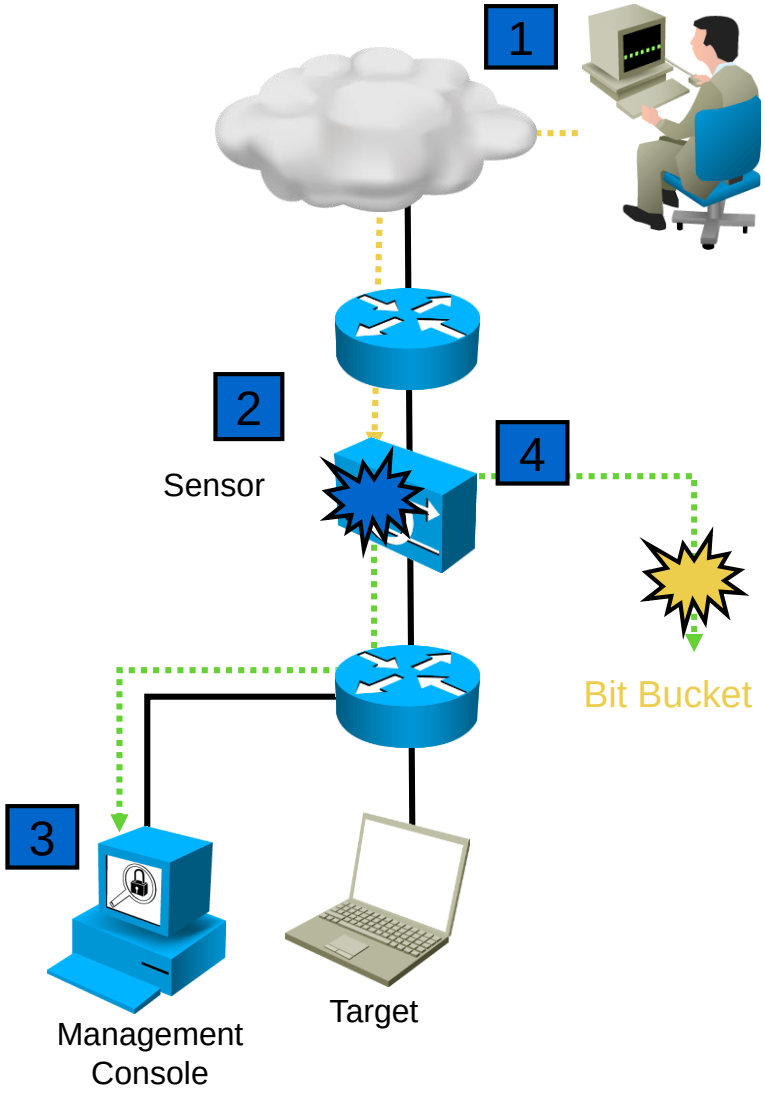
Intrusion Detection Systems (IDSs)



1 Tổng quan về IDS/IPS

- **Intrusion Prevention System:** là một hệ thống bao gồm cả chức năng phát hiện xâm nhập (Intrusion Detection – ID) và khả năng ngăn chặn các xâm nhập trái phép vào tài nguyên của hệ thống mạng

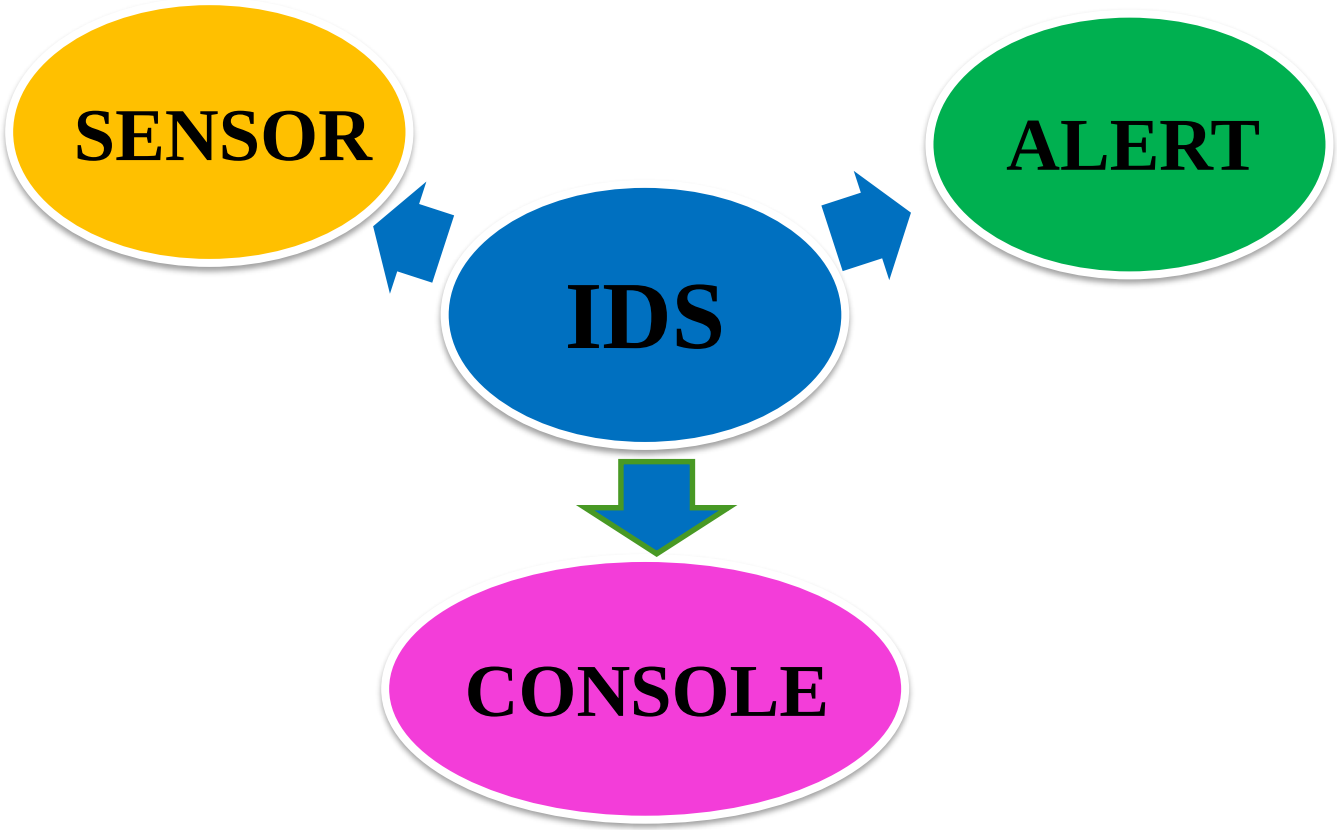
Intrusion Prevention Systems (IPSs)



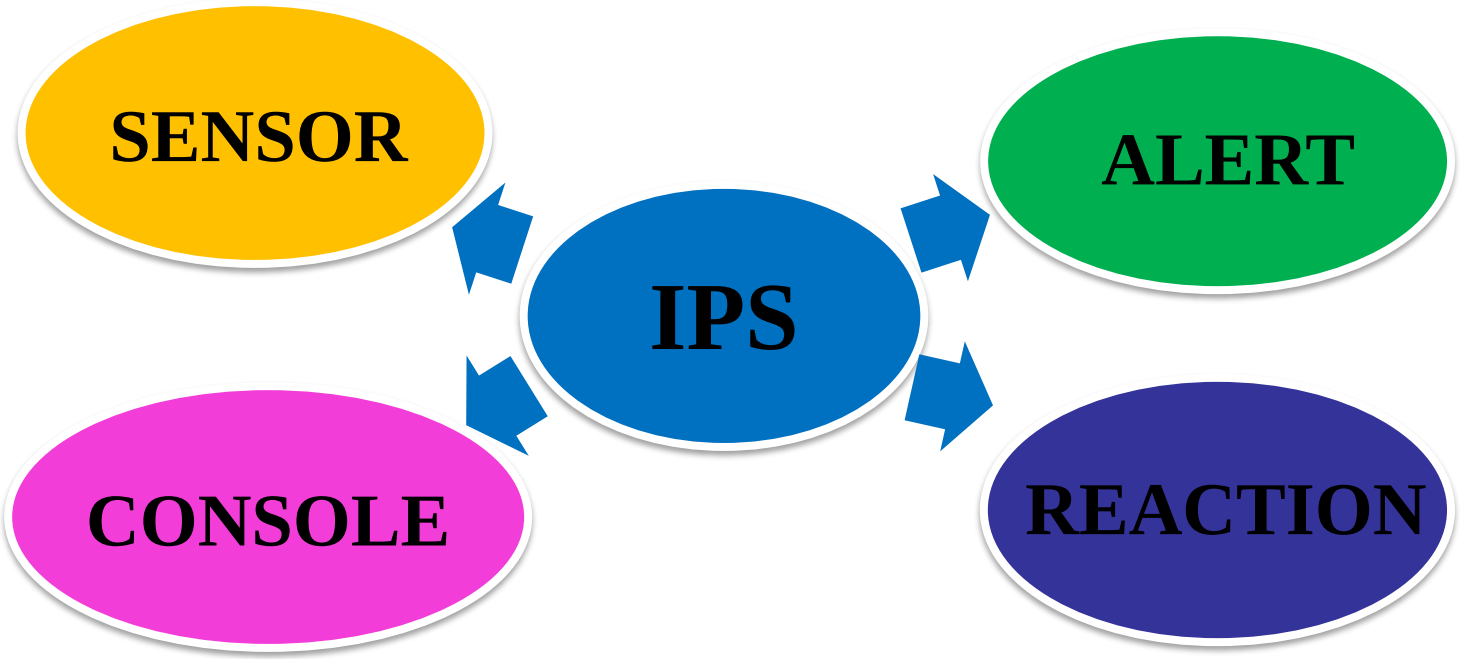
Nội dung

1. Tổng quan về IDS/IPS?
2. Thành phần chính của IDS/IPS?
3. Phân loại IDS/IPS ?
4. Các kỹ thuật phát hiện xâm nhập
5. Snort

2 Thành phần chính của IDS/IPS



2 Thành phần chính của IDS/IPS

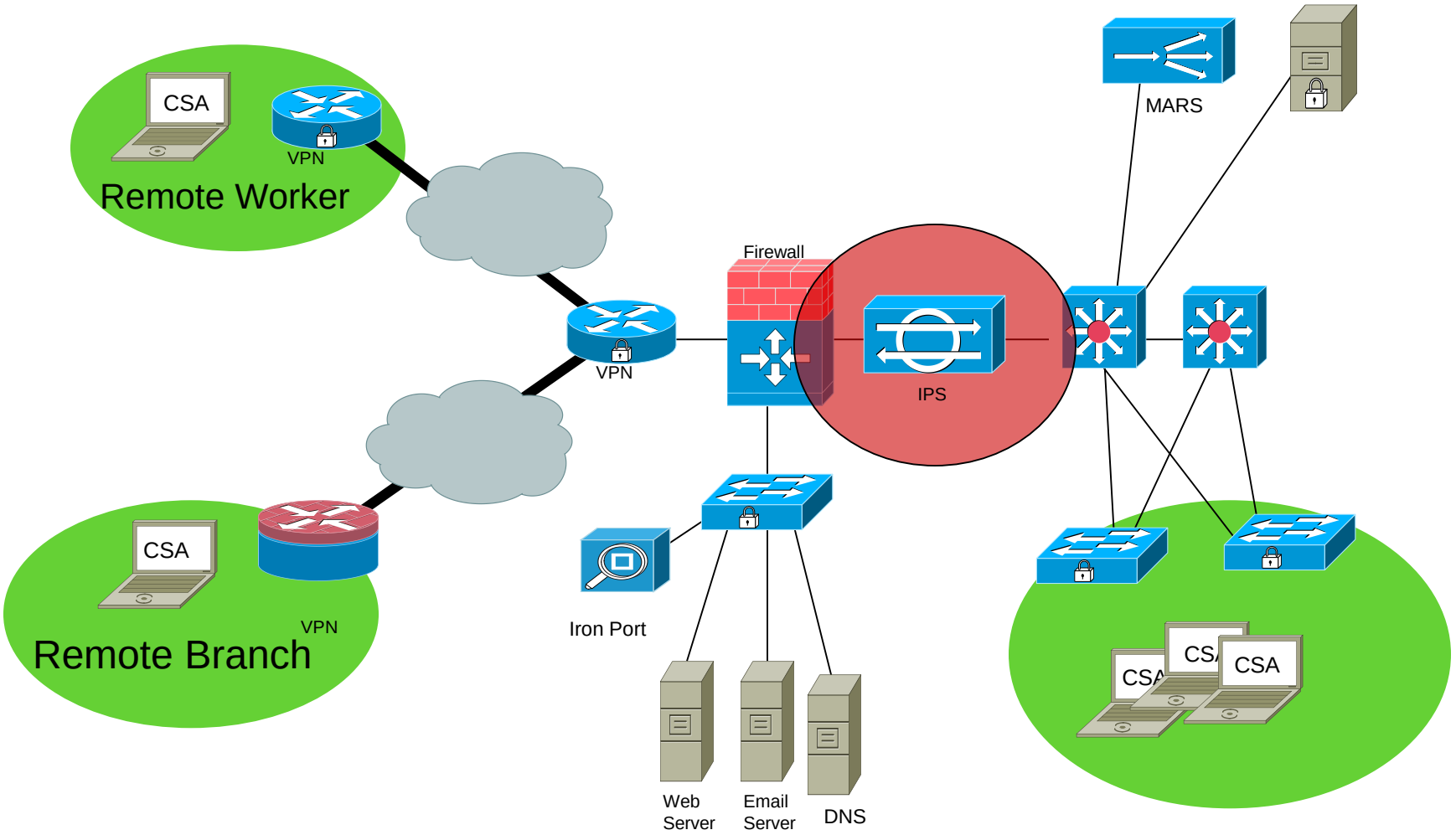


Nội dung

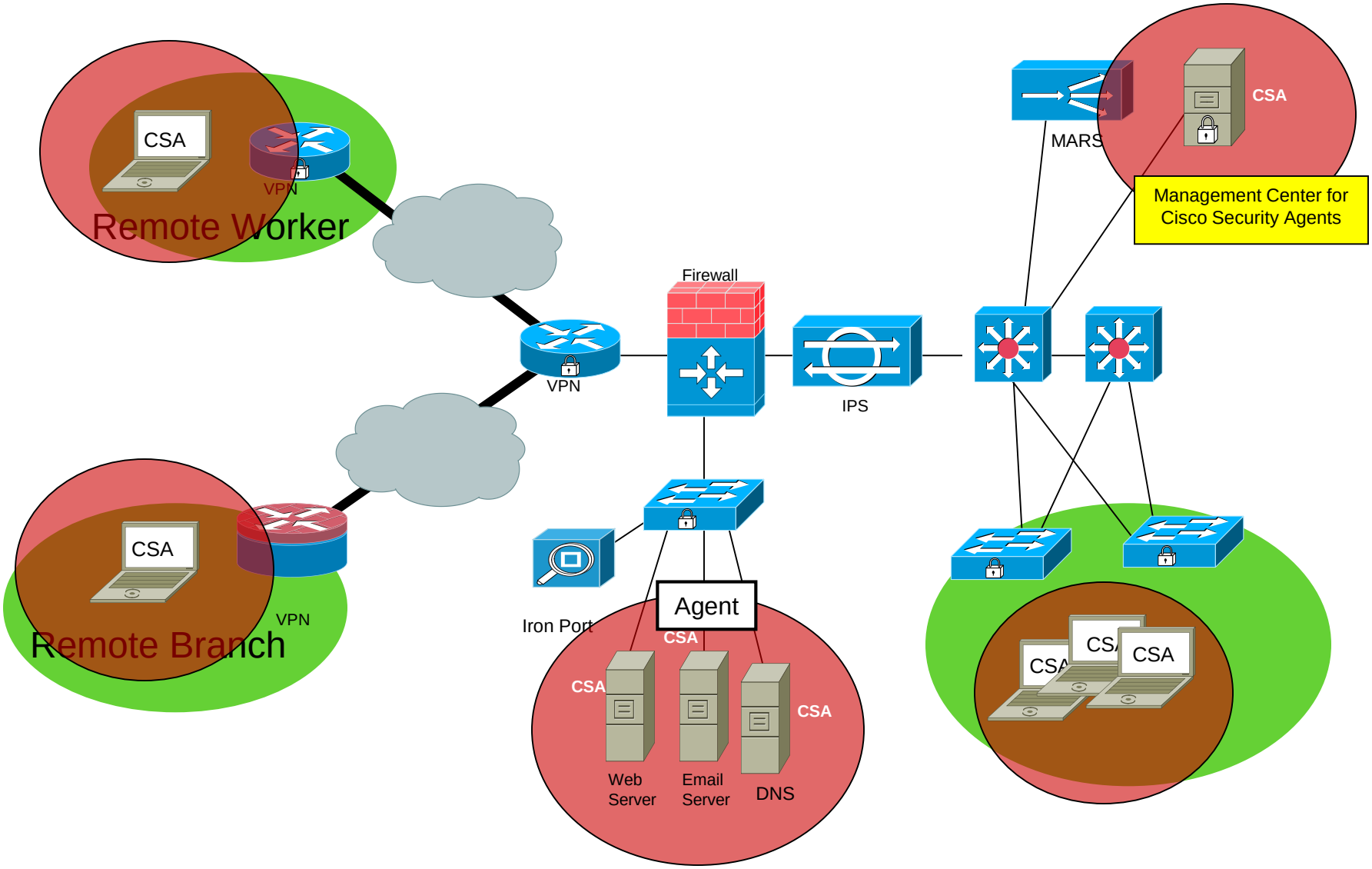
1. Tổng quan về IDS/IPS?
2. Thành phần chính của IDS/IPS?
3. Phân loại IDS/IPS ?
4. Các kỹ thuật phát hiện xâm nhập
5. Snort

3 Phân loại IDS/IPS

Network-Based



Host-Based


CSA
VPN
Remote Worker
MARS
CSA
Management Center for
Cisco Security Agents
Firewall
VPN
IPS
CSA
VPN
Remote Branch
Iron Port
Agent
CSA
CSA
CSA
CSA
Web
Server
Email
Server
DNS
CSA
CSA

Nội dung

1. Tổng quan về IDS/IPS?
2. Thành phần chính của IDS/IPS?
3. Phân loại IDS/IPS ?
4. Các kỹ thuật phát hiện xâm nhập
5. Snort

4 Các kỹ thuật phát hiện xâm nhập

1

Signature-based

Dựa vào cơ sở dữ liệu có sẵn để so sánh và phát hiện ra các cuộc tấn công

2

Anomaly-based

Dựa vào hoạt động trên mạng và so sánh với luồng traffic đã được học trước để biết hành động đó là bình thường hay bất thường

3

Stateful Protocol Analysis

Yếu tố chính của hệ thống IDPS. Giao thức phân tích và giải nén gói tin trên mạng

Nội dung

1. Tổng quan về IDS/IPS?
2. Thành phần chính của IDS/IPS?
3. Phân loại IDS/IPS ?
4. Các kỹ thuật phát hiện xâm nhập
5. Snort

Snort

- Giới thiệu về Snort
- Cấu trúc của Snort
- Các Module của Snort
- Bộ luật của Snort
- Chế độ ngăn chặn của Snort: Snort - Inline

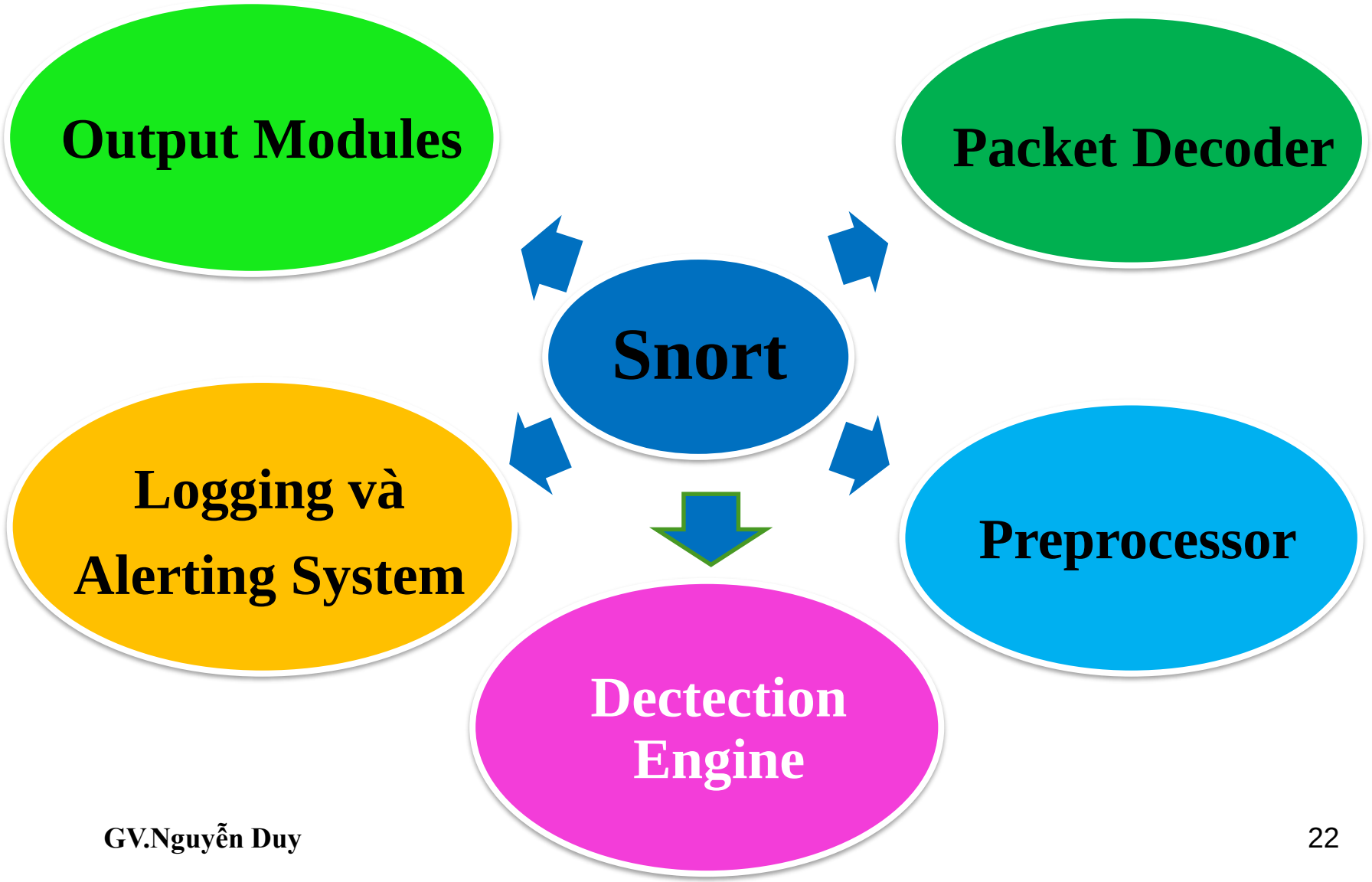
5 Giới thiệu về Snort

- Snort là một hệ thống phát hiện xâm nhập mạng (NIDS) mã nguồn mở miễn phí.
- Dữ liệu được thu thập và phân tích bởi Snort. Snort lưu trữ dữ liệu bằng cách dùng output plug-in.
- Snort sử dụng các luật được lưu trữ trong các file text, có thể được chỉnh sửa bởi người quản trị.
- Các luật được nhóm thành các kiểu.

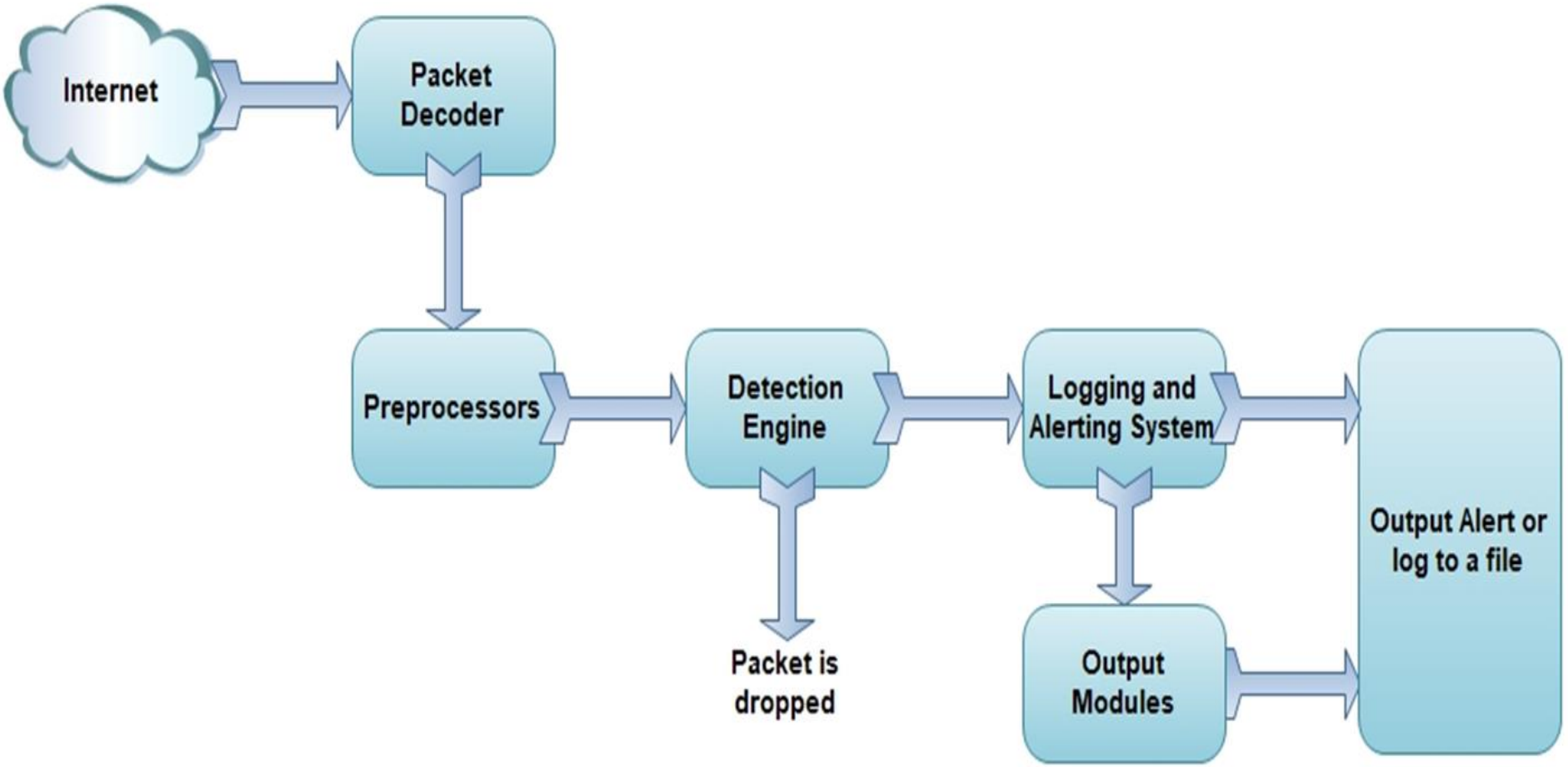
5 Giới thiệu về Snort

- Snort bao gồm 1 hoặc nhiều Sensor và 1 server CSDL chính. Các Sensor có thể đc đặt trước hoặc sau firewall:
  - Trước: giám sát các cuộc tấn công vào firewall và hệ thống mạng.
  - Sau: ghi nhớ các cuộc vượt firewall thành công.

5 Cấu Trúc của Snort



5 Các Module của Snort



5 Các Module của Snort

- **Packet Decoder:** Snort sử dụng thư viện pcap để bắt mọi gói tin trên mạng lưu thông qua hệ thống và giải mã chúng.

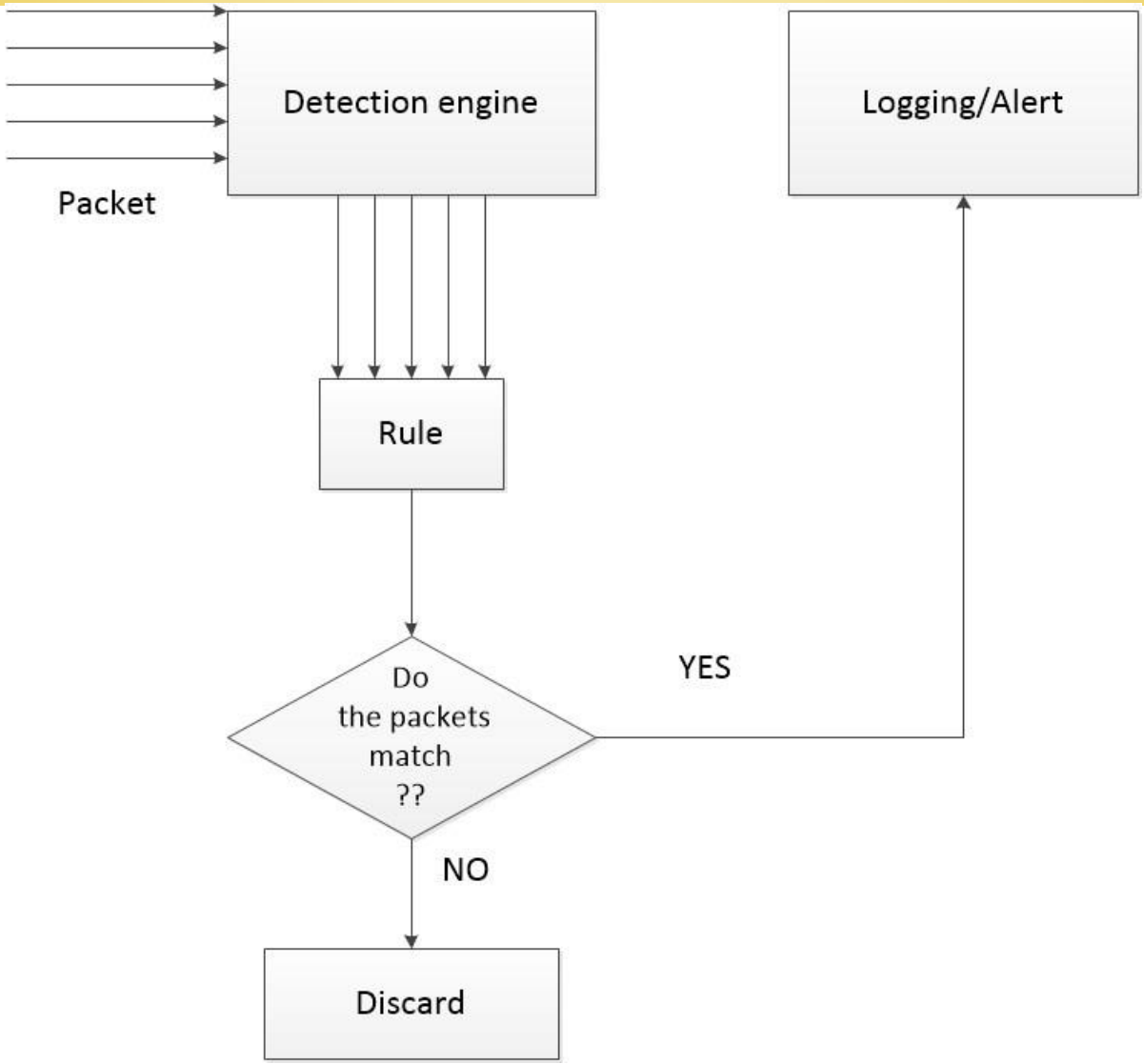
5 Các Module của Snort

- **Preprocessor:** Là module quan trọng của Snort, chuẩn bị gói dữ liệu cho modue Detection Engine. Có 3 nhiệm vụ chính:
  - Kết hợp lại các gói tin.
  - Giải mã và chuẩn hóa các giao thức.
  - Phát hiện xâm nhập bất thường.

5 Các Module của Snort

- **Detection Engine**: Đây là module quan trọng nhất của Snort. Nó chịu trách nhiệm phát hiện các dấu hiệu xâm nhập. Môđun phát hiện sử dụng các rule định nghĩa trước để so sánh với dữ liệu thu thập được từ đó xác định xem có hợp lệ hay không.

Các Module của Snort

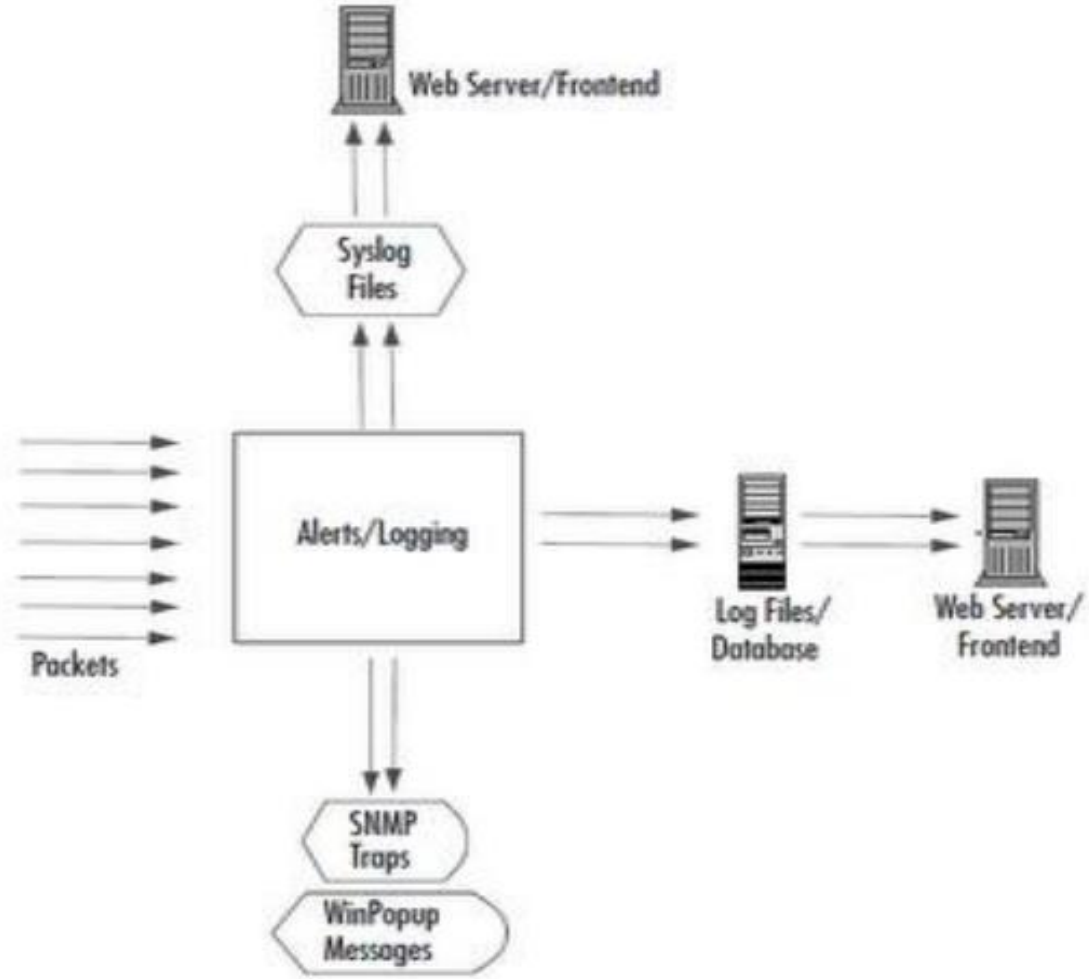


5 Các Module của Snort

- **Logging và Alerting System:** Tùy thuộc vào module Detection Engine có phát hiện được xâm nhập hay không mà gói tin có thể bị ghi log hoặc đưa ra cảnh báo. Các file log là các file text dữ liệu, có thể được lưu dưới nhiều định dạng khác nhau

Các Module của Snort

Output Module



5 Bộ Luật của Snort

- Snort hoạt động dựa trên các luật.
- Các luật của Snort được lưu trong các file text, có thể được chỉnh sửa bởi người quản trị.
- Dựa vào các thông tin, dấu hiệu riêng từ các hành động xâm phạm để tạo ra rule cho snort.
- Một luật có thể được sử dụng để tạo ra một thông điệp cảnh báo, ghi lại một thông điệp
- Các luật thường được đặt trong file cấu hình, thường là **snort.conf**. Bạn cũng có thể sử dụng nhiều file bằng cách gom chúng lại trong một file cấu hình chính.

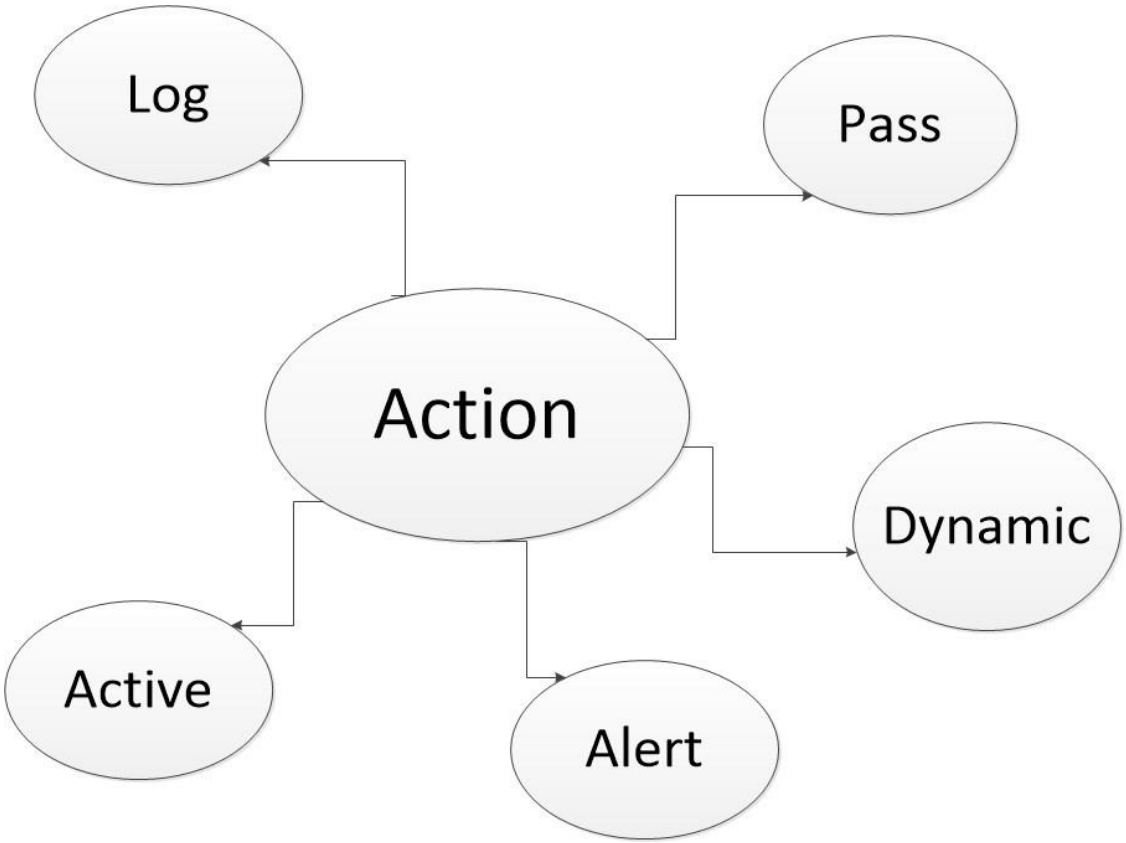
5 Cấu Trúc của Rule

alert tcp 192.168.2.0/24 23 -> any any (content: “confidential”; msg: “Detected confidential”)

Action	Protocol	Address	Port	Direction	Address	Port
alert	tcp	192.168.2.0/24	24	->	any	any

Chi tiết Rule Header

5 Cấu Trúc của Rule



5 Cơ chế Snort Inline

- Ý tưởng chính của inline-mode là kết hợp khả năng ngăn chặn của iptables vào bên trong snort. Điều này được thực hiện bằng cách thay đổi môđun phát hiện và môđun xử lý cho phép snort tương tác với iptables.
- Đưa thêm 3 hành động DROP, SDROP, INJECT và thay đổi trình tự ưu tiên của các luật trong Snort

Question ???