



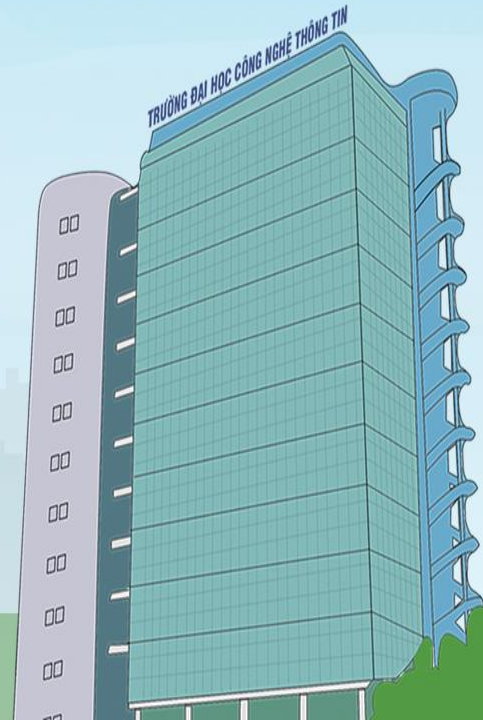
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
Khoa Mạng máy tính & Truyền thông

Network-based IDS (tt)

NT204 – Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GV: Đỗ Hoàng Hiễn

hiendh@uit.edu.vn





Nội dung hôm nay...

Network-based IDPS

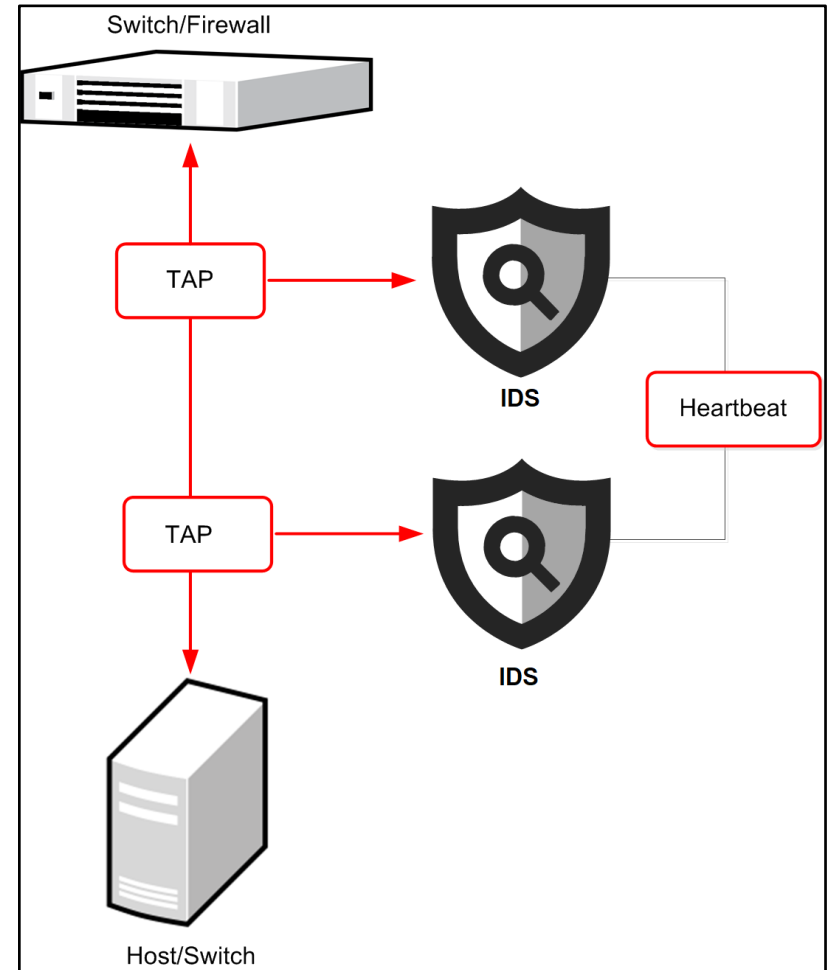
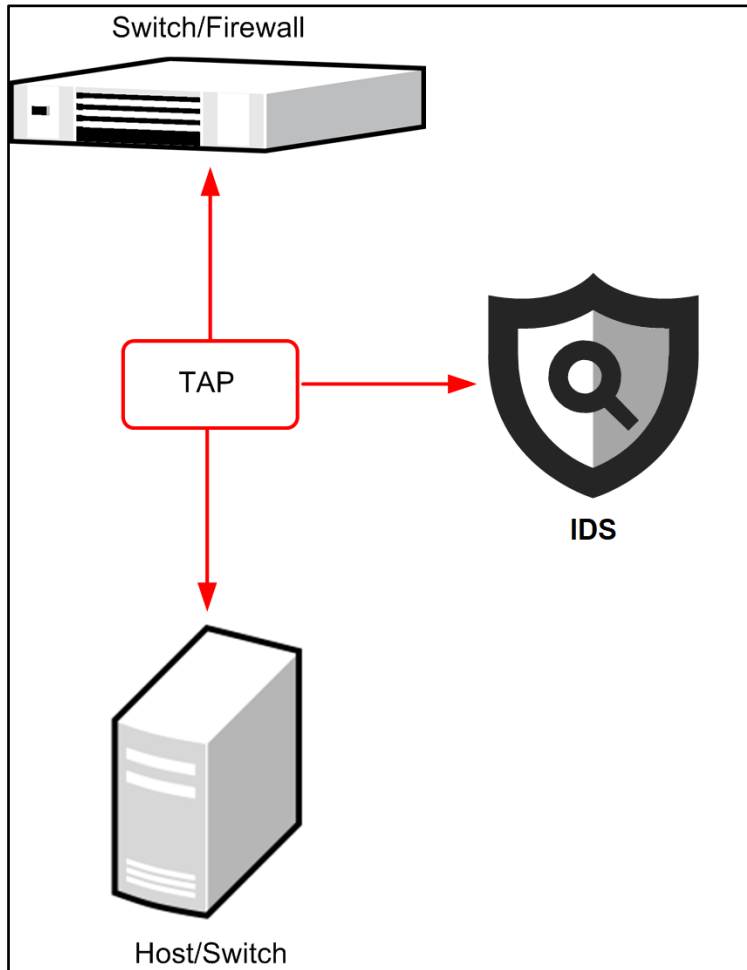
**Hôm nay có gì?
VD triển khai NIDPS
Snort**

Tài liệu:

- NIST, Chapter 4

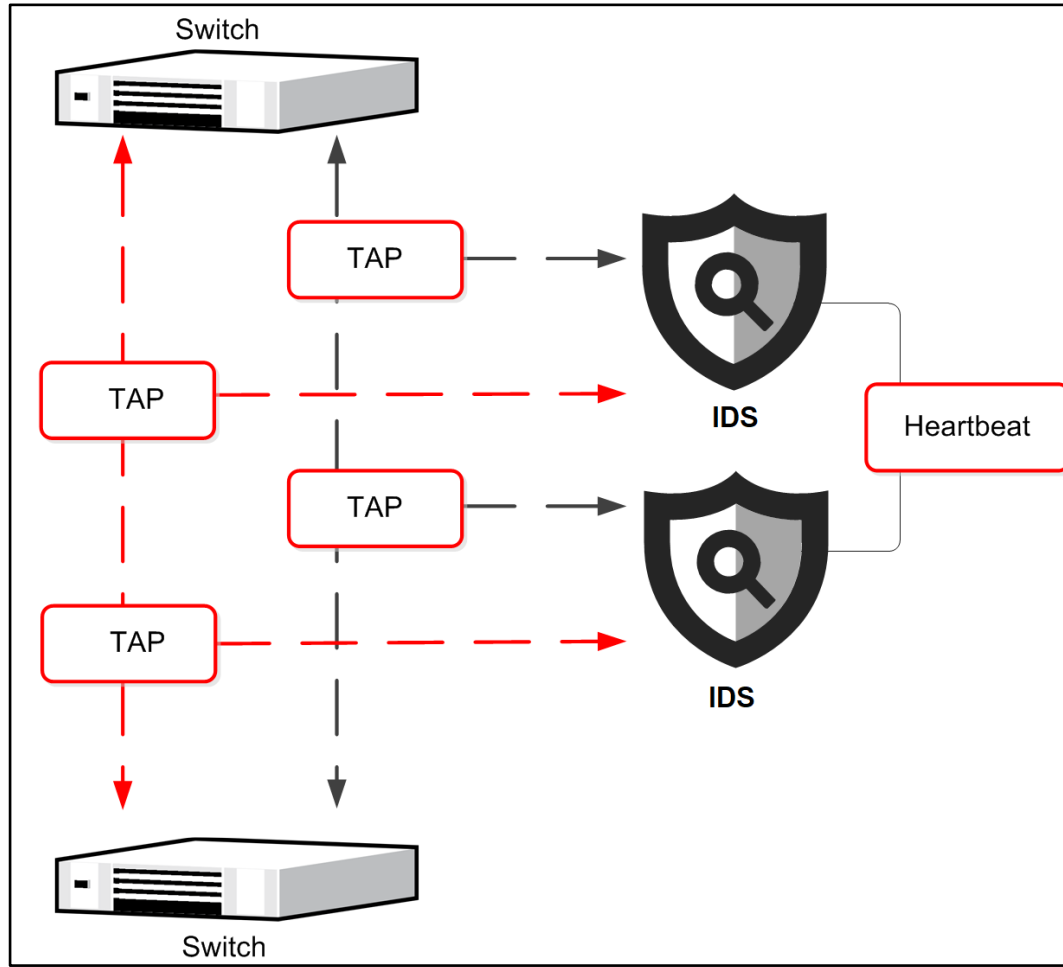
Triển khai IDS

VD: Triển khai IDS với network TAP



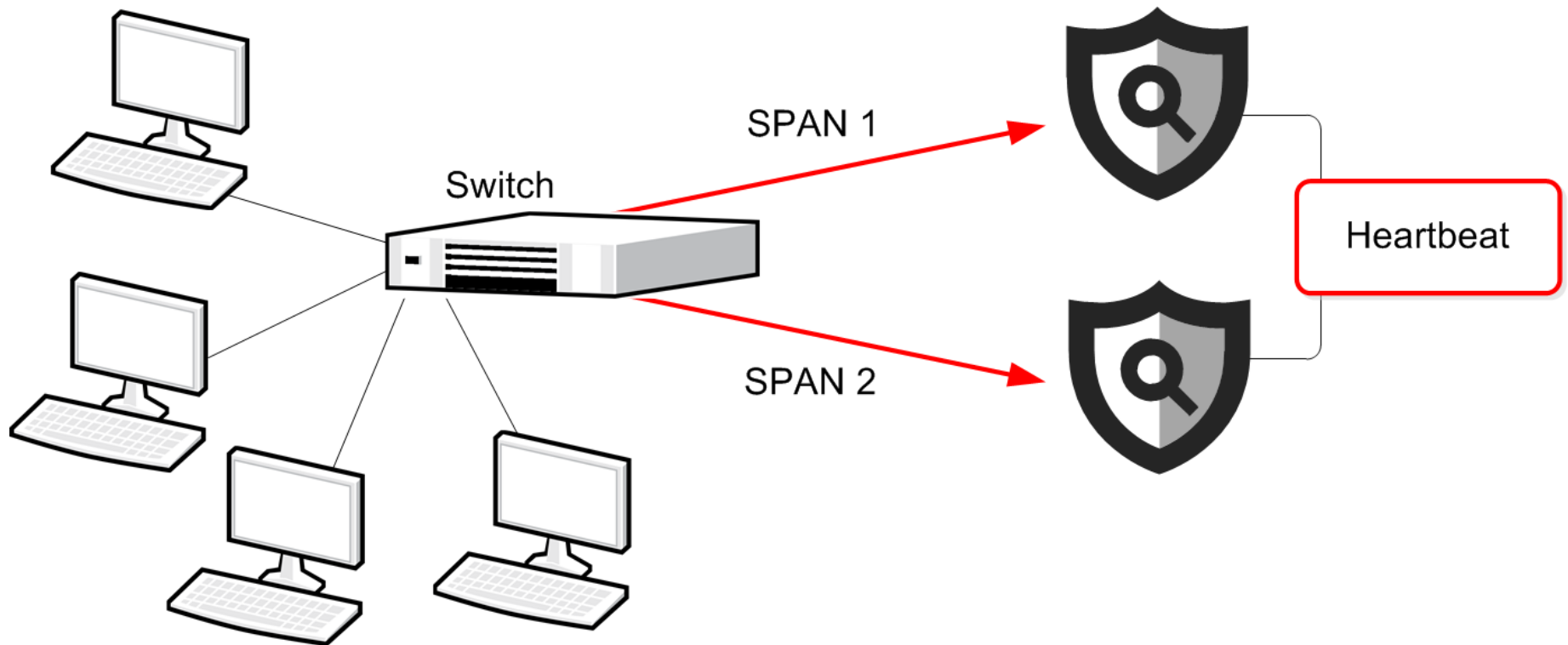
Triển khai IDS

VD: Triển khai IDS với network TAP



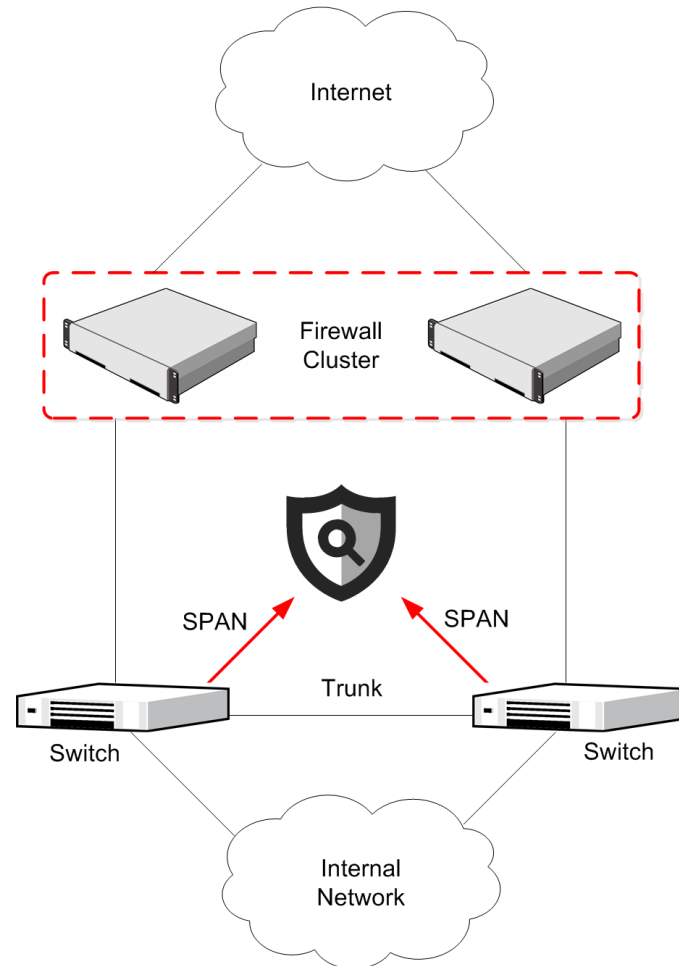
Triển khai IDS

VD: Triển khai IDS với Port mirroring



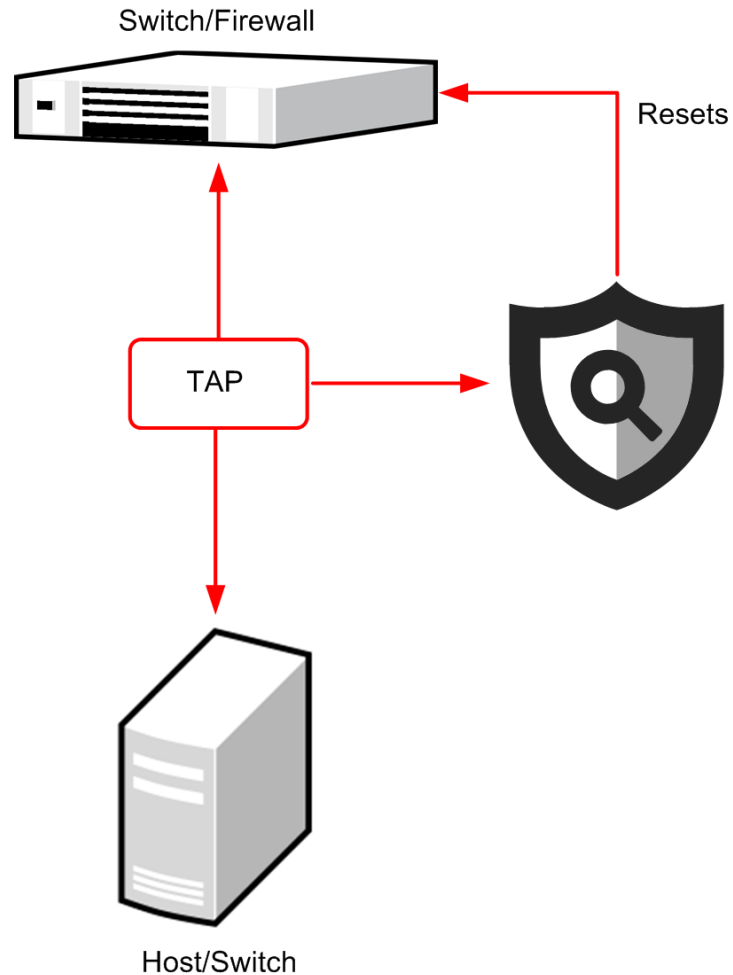
Triển khai IDS

VD: Triển khai IDS với Port mirroring



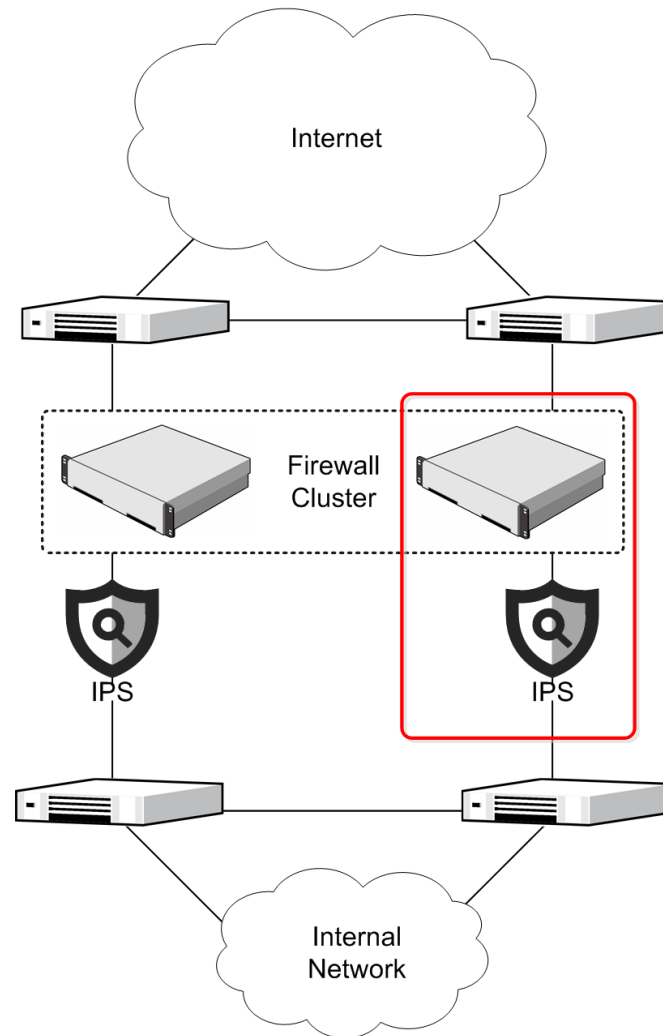
Triển khai IDS

VD: Triển khai IDS với Reset Interface



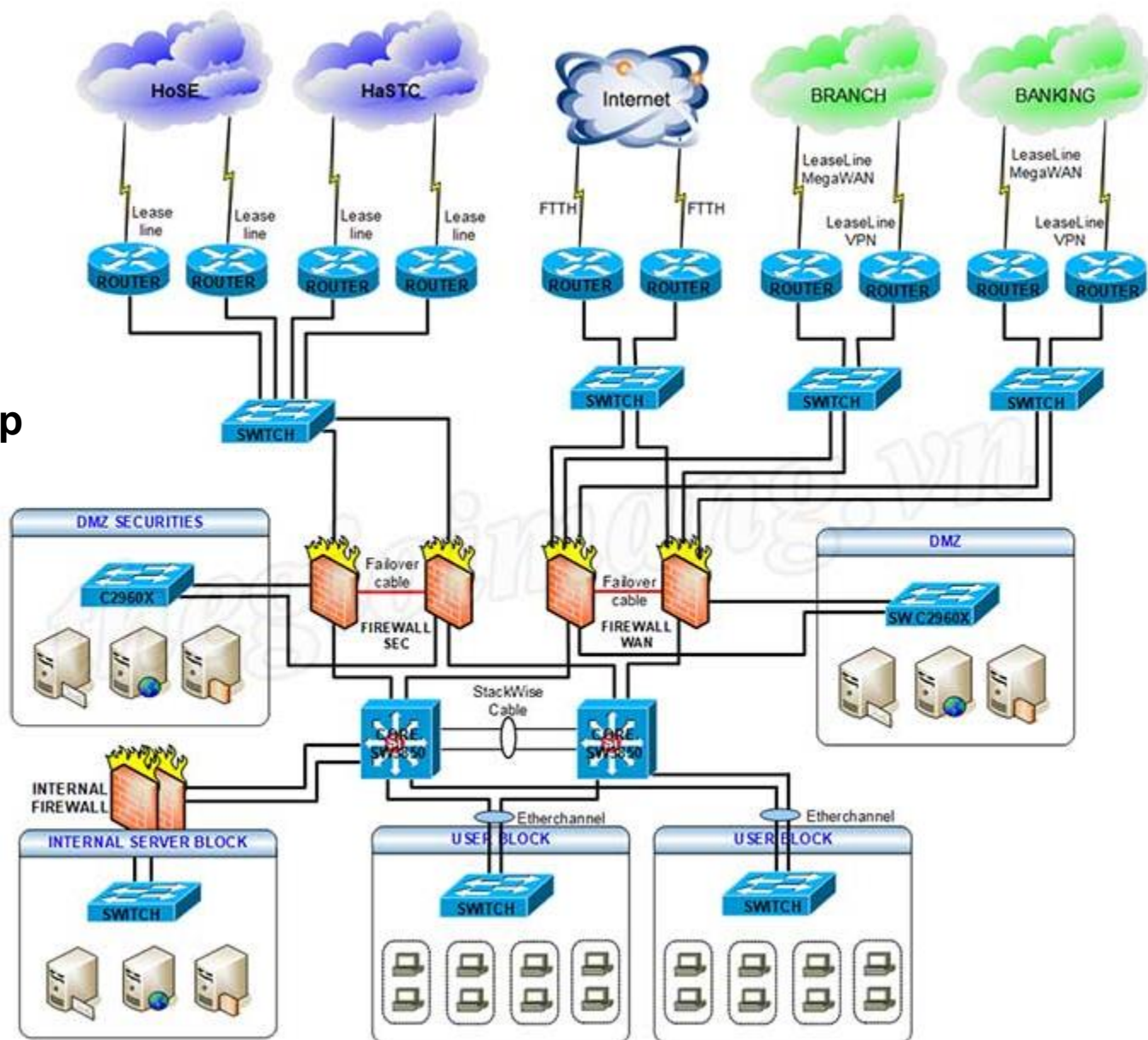
Triển khai IPS

VD: Triển khai IPS trong inline mode



Triển khai IDPS Vận dụng

Đặt các NIDS/NIPS
tại các vị trí phù hợp



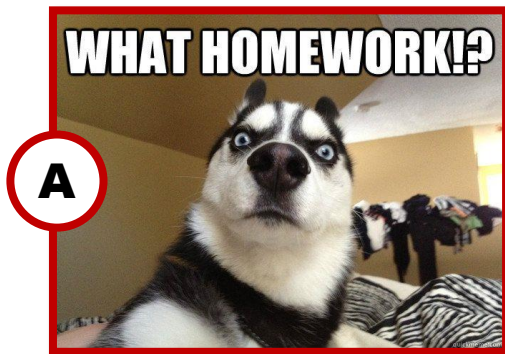
Nhắc lại

Assignment 1: Cài đặt Snort

Câu hỏi:



Trả lời:



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 1: Snort thuộc loại NIDPS nào?

- A** Signature-based NIDPS
- B** Anomaly-based NIDPS
- C** Specification-based NIDPS
- D** Hybrid NIDPS



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 2: Snort có thể làm gì? *(Có thể chọn nhiều đáp án)*

- A** Bắt lưu lượng mạng đang truyền
- B** Phân tích các gói tin mạng thu thập được
- C** Ghi log các sự kiện, thông tin
- D** Nhận diện tấn công



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 3: Snort sử dụng ... cho việc nhận diện tấn công.

- A** Một cơ sở dữ liệu tấn công đính kèm
- B** Một mô hình máy học phân loại lưu lượng bình thường hay tấn công
- C** Một tập các bộ rules định nghĩa dấu hiệu của tấn công
- D** Đáp án khác

Nhắc lại

Tìm hiểu về Snort

Câu hỏi 4: Có thể truy cập vào các rules định nghĩa tấn công của Snort bằng cách nào?

- A** Snort cung cấp các tập rule mặc định kèm theo trong source cài đặt
- B** Người dùng có thể tự viết các rule của Snort
- C** Có nhiều tập rule dành cho các người dùng khác nhau trên trang chủ
- D** Cách nào cũng được 😊



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 5: Snort có thể nhận lưu lượng mạng để phân tích từ nguồn nào?

- A** Lưu lượng mạng bắt được trên interface giám sát
- B** Từ 1 file pcap chứa lưu lượng mạng đã bắt trước đó
- C** Snort cần hết cả 2 nguồn trên 😊
- D** Chưa



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 6: Snort có cho phép chặn tấn công hay không?

- A** Mặc định là có
- B** Không
- C** Có nhưng chỉ ở chế độ phù hợp
- D** Chưa làm thử bao giờ



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 7: Phiên bản Snort mà nhóm đã cài?

- A** Version 2
- B** Version 3
- C** Chỉ có Version 1. Đúng nhận sai cãi.
- D** Ủa, Snort có phiên bản khác nhau????



Nhắc lại

Tìm hiểu về Snort

Câu hỏi 8: Đã thử tự viết 1 rule Snort đơn giản chưa 😊?

- A** Dạ rồi
- B** Dạ chưa
- C** Em thành master về rule rồi 😎
- D** Chưa cài Snort

Snort

- **Snort là gì?**

- Là một NIDPS mã nguồn mở
- Signature-based NIDPS

- **Khả năng của Snort**

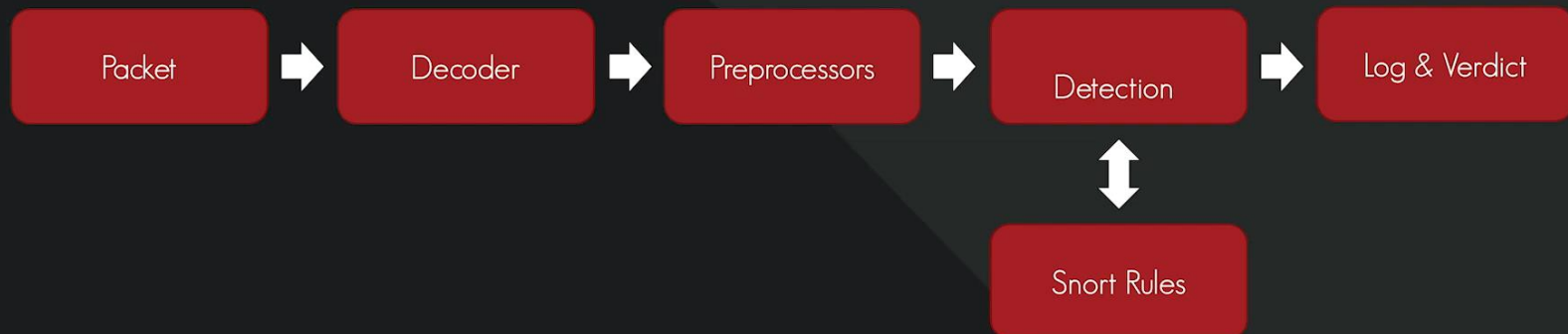
- Phân tích lưu lượng mạng theo thời gian thực
- Ghi log các gói tin
- Phân tích giao thức, tìm kiếm/so khớp nội dung
- Phát hiện tấn công hoặc do thám dựa trên các rules và các thông tin phân tích được



Quy trình phân tích gói tin

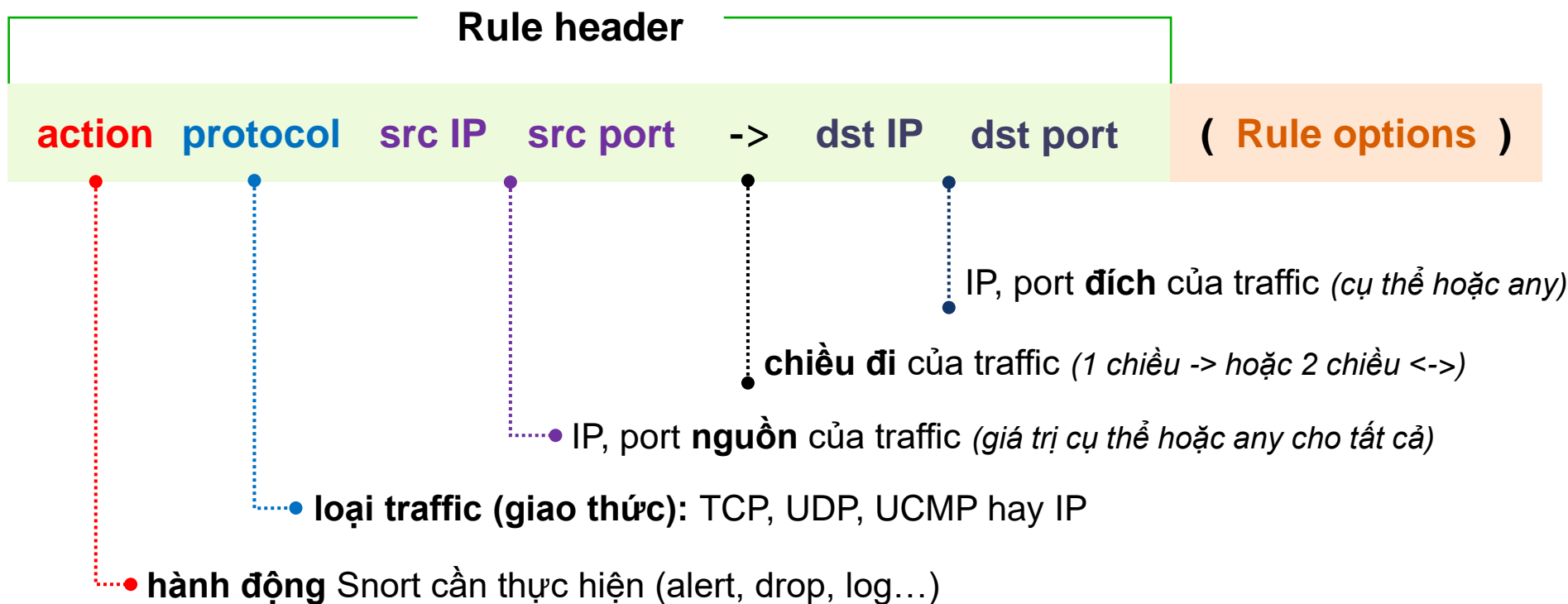
Snort 2

Life of a Packet



Snort 2 rules

- Định nghĩa **các sự kiện/điều kiện** mà Snort cần quan tâm, ví dụ như một tấn công, và **hành động nên thực hiện** khi sự kiện xảy ra
- Các file **.rules**



Snort 2 rules

• Rule options

- Là phần trọng tâm trong khả năng phát hiện tấn công của Snort
- Chia là nhiều nhóm option, quan trọng nhất là các **detection options** dùng để phát hiện tấn công
- Mỗi option có dạng
key : tham số 1[, tham số 2]
- Các option phân cách với nhau bằng ;

EXAMPLE	
Rule Header	<code>alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any</code>
Message	<code>msg: "BROWSER-IE Microsoft Internet Explorer CacheSize exploit attempt";</code>
Flow	<code>flow: to_client,established;</code>
Detection	<code>file_data; content:"recordset"; offset:14; depth:9; content:".CacheSize"; distance:0; within:100; pcrc:"/CacheSize\s*=\s*/"; byte_test:10,>,0x3fffffff,0,relative,string;</code>
Metadata	<code>policy max-detect-ips drop, service http;</code>
References	<code>reference:cve,2016-8077;</code>
Classification	<code>classtype: attempted-user;</code>
Signature ID	<code>sid:65535;rev:1;</code>

Snort 2 rules: Ví dụ 1

```
alert icmp any any -> 192.168.1.1 any (msg: "ICMP detected"; sid: 100005)
```

- **Đặc điểm traffic**
 - Giao thức: ICMP
 - Nguồn: tất cả IP và port
 - Đích: tất cả các port của 192.168.1.1
- **Hành động của Snort**
 - Hành động cần thực hiện: cảnh báo (alert)
 - Thông điệp sẽ cảnh báo: ICMP detected
 - ID của rule: 100005

Kết luận:

Snort hiện thông điệp cảnh báo **"ICMP detected"** khi phát hiện có bất kỳ host nào ping tới 192.168.1.1

Snort 2 rules: Ví dụ 2

```
alert tcp 192.168.1.0/24 21 -> any any
```

(msg: "FTP failed login"; content: "Login or password incorrect"; sid: 100007)

- **Đặc điểm traffic**

- Giao thức: TCP
- Nguồn: port 21 từ các IP trong subnet 192.168.1.0/24
- Đích: tất cả các port và IP khác
- Nội dung traffic có chứa "**Login or password incorrect**" (là thông điệp gửi từ FTP server → client)

- **Hành động của Snort**

- Hành động cần thực hiện: cảnh báo (alert)
- Thông điệp sẽ cảnh báo: FTP failed login
- ID của rule: 100007

Kết luận:

Snort hiện thông điệp cảnh báo "**FTP failed login**" khi phát hiện có bất kỳ client nào đăng nhập sai khi kết nối với FTP server trong subnet 192.168.1.0/24

Snort 2 rules: Ví dụ 3

```
alert tcp $EXTERNAL_NET any -> any $HTTP_PORTS
```

snort.conf

```
(msg: "XSS"; content: "<script>";  
flow:to_server,established; sid: 100009)
```

- **Đặc điểm traffic**

- Giao thức: TCP
- Nguồn: từ bất kỳ port nào và các IP định nghĩa trong \$EXTERNAL_NET
- Đích: tất cả các IP, các port định nghĩa trong \$HTTP_PORTS
- Nội dung traffic có chứa “<script>”
- Chỉ xét traffic client gửi đến server sau khi kết nối TCP đã được thiết lập

- **Hành động của Snort**

- Hành động cần thực hiện: cảnh báo (alert)
- Thông điệp sẽ cảnh báo: XSS
- ID của rule: 100009

Kết luận:

Snort hiện thông điệp cảnh báo “**XSS**” khi phát hiện có bất kỳ client nào ở mạng ngoài gửi request có chứa “<script>” cho web servers

Cần thông tin gì để viết rule?

- Xác định được đặc điểm để lọc traffic cho sự kiện cần kiểm tra:

- Giao thức
 - Nguồn, đích (IP và port)
 - Trong content có chứa gì đặc biệt?
 - Kích thước có điểm gì đặc biệt? (ví dụ rất lớn, rất nhỏ, 0...)
 - ...
- } rule header

→ *phải có hiểu biết về sự kiện/tấn công*

- Hành động của Snort

- Cảnh báo/Drop/Ghi log
- ID cho rule
- Phân loại cho sự kiện

Today end,
**See you
next week!**

