



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

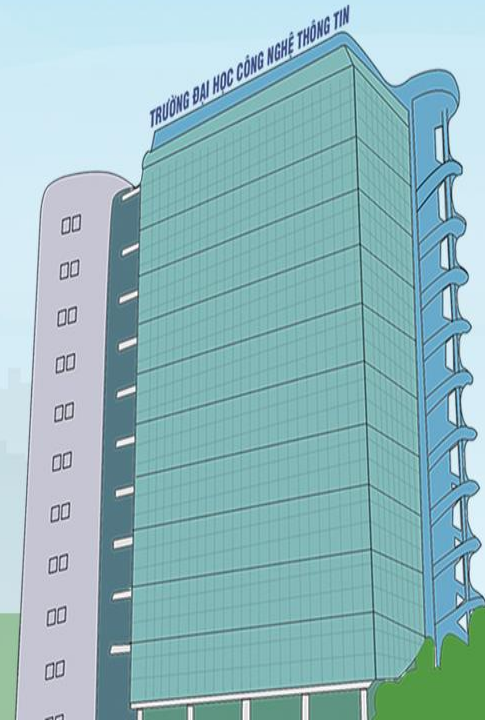
# Giới thiệu môn học

---

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

GV: Đỗ Hoàng Hiễn

[hiendh@uit.edu.vn](mailto:hiendh@uit.edu.vn)





## Hôm nay học gì?

1. Giới thiệu môn học
2. Giới thiệu về IDS/IPS

# Nội dung

Tổng quan về IDS/IPS

# Thông tin môn học

Giới thiệu môn học

## ***Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập*** ***Intrusion Detection and Prevention System (IDS/IPS - IDPS)***

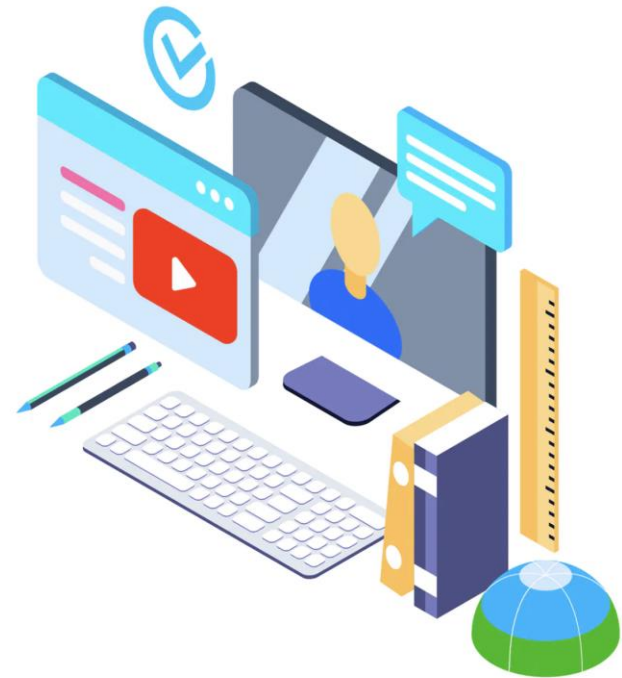
- SV cần các kiến thức nền tảng:
  - Nguyên tắc hoạt động cơ bản của mạng máy tính (IT005)
  - Cơ bản về các tấn công mạng và phương pháp phòng thủ (NT101)
  - Kiến thức về hệ điều hành Linux, Windows
  - Kỹ năng nghiên cứu cơ bản (đọc hiểu, phân tích, cài đặt/cấu hình)
  - Kiến thức về Machine Learning / Deep Learning



# Quản lý khoá học

## Giới thiệu môn học

- Website môn học: <https://courses.uit.edu.vn/>
  - Thông báo
  - Thông tin khoá học, các quy định
  - Bài giảng, tài liệu tham khảo
  - Bài tập, bài thực hành



# Mục tiêu môn học

## Giới thiệu môn học

Sau khi kết thúc môn học, sinh viên có thể:

- Hiểu được cơ bản các vấn đề, khái niệm, phân loại, nguyên tắc hoạt động và các kỹ thuật trong các hệ thống IDPS.
- Hiểu được lúc nào, ở đâu, bằng cách nào và lý do khi áp dụng các công cụ IDPS và các kỹ thuật liên quan để đảm bảo an toàn mạng.
- Tiếp cận các hướng mới cho IDPS (học máy/học sâu) và cách áp dụng các công nghệ bảo mật mới vào kiến trúc mạng hiện có.
- Có thể triển khai, đánh giá, tùy chỉnh một IDPS cho những yêu cầu bảo mật cụ thể.

**Hint:** Nhiều bài tập vận dụng, bài tập nghiên cứu được dùng để đánh giá các **mục tiêu môn học** này!



# Giáo trình, tài liệu

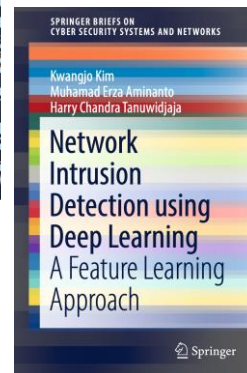
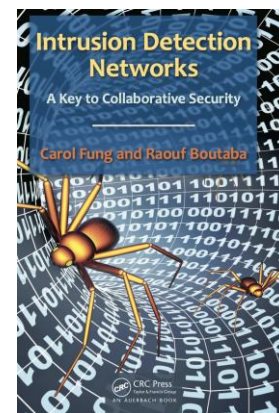
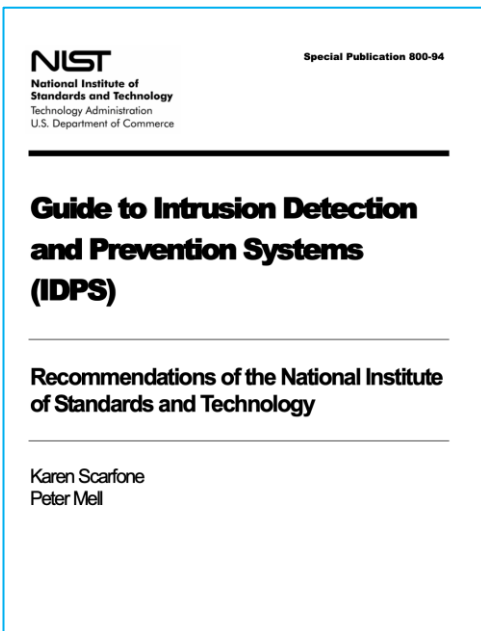
Giới thiệu môn học

## ○ Giáo trình:

- **Không có giáo trình!**
- **Nội dung môn học dựa trên một số bài báo khoa học gần đây trong nhiều hội nghị hoặc tạp chí chuyên ngành; các hướng dẫn và tài liệu của các công cụ IDPS**

## Tài liệu tham khảo thêm:

- Karen Scarfone and Peter Mell, **Guide to Intrusion Detection and Prevention Systems (IDPS)**, *Recommendations of the National Institute of Standards and Technology*, 2007
- Carol Fung and Raouf Boutaba, **Intrusion Detection Networks - A Key to Collaborative Security**, CRC Press, 2013
- Một số bài báo khoa học liên quan (sẽ được cung cấp tương ứng trong các buổi học)



# Nội dung từng tuần (dự kiến)

Giới thiệu môn học

Tuần 1: **Giới thiệu môn học**

Tuần 2: **Ôn tập về tấn công mạng, tổng quan IDPS**

Tuần 3 - 4: **Network-based IDPS**

Tuần 5: **Host-based IDPS**

Tuần 6: **Security Monitoring, Log analysis, SIEM/SOC**

Tuần 7: **Báo cáo đồ án lần 1 (Giữa kỳ)**

Tuần 8: **Đánh giá và đánh lừa IDPS**

Tuần 9 – 10: **Học máy cho IDS**

Tuần 11: **Bảo mật cho Học máy**

Tuần 12 – 15: **Báo cáo đồ án lần 2 (cuối kỳ)**





# Đánh giá

Giới thiệu môn học

**30%** quá trình + **20%** thực hành + **50%** cuối kỳ

## ○ Quá trình

- Điểm danh, câu hỏi trên lớp, các bài tập nghiên cứu tài liệu
- Bài tập về nhà
- Đồ án môn học

## ○ Không thi giữa kỳ

## ○ Đồ án

- Thực hiện theo nhóm
- Danh sách chủ đề và thông tin đăng ký đồ án sẽ thông báo sau

## ○ Cuối kỳ

- Thi cuối kỳ: gồm trắc nghiệm và tự luận (nội dung gồm LT, TH, BT)





# Yêu cầu

## Giới thiệu môn học

### ○ Quy định trong lớp:

- Đến lớp đúng giờ. Có thể ghi nhận điểm (*cộng/trừ điểm danh hoặc cộng điểm các bài tập/quiz trên lớp*)
- Không làm việc riêng trong giờ học, không sử dụng điện thoại hoặc laptop vào để làm các việc không liên quan đến nội dung buổi học

### ○ Phòng ngừa dịch bệnh và nghỉ học:

- Đeo khẩu trang và giữ khoảng cách khi có dấu hiệu cảm cúm, bệnh truyền nhiễm...
- Nghỉ học cần gửi email cho GV trước buổi học. Tiêu đề email phải có mã lớp



# Một số điểm cần lưu ý

## Giới thiệu môn học

### ○ Luôn trung thực, cố gắng

- Trung thực trong quá trình học – *Đừng dễ bị cám dỗ*
- Các bài nộp cần đảm bảo là **100% công sức** của chính mình, cần **trích dẫn rõ ràng** các nguồn tài liệu đã tham khảo
- *Nộp bài làm mà mình cảm thấy hài lòng* – đừng làm ẩu hay lười biếng!
- Bị **0 điểm** (môn học) cho bất kỳ hành vi nào liên quan đến việc **gian lận** hoặc **sao chép**
- **Không “thử nghiệm”** với các hệ thống không được phép
- Bị **0 điểm** nếu **vắng hơn 50% buổi học** (TH: > 3/6 buổi, QT: hơn 1 nửa số lần điểm danh trên lớp)



# Một số điểm cần lưu ý

Giới thiệu môn học

## ○ Tìm tòi và thực nghiệm

- Các hoạt động thực nghiệm cần sử dụng container hoặc máy ảo
- **Nhắc lại:** Chỉ thực nghiệm trên các hệ thống được cho phép



**Không chia sẻ các tài liệu học** (*slides, assignments, labs, ...*) **ra ngoài lớp học**  
**mà không có sự cho phép của GV!**

*Chỉ lưu hành nội bộ*

# Liên hệ Giảng viên

Giới thiệu môn học

- **Best way!!** Gửi email đến [hiendh@uit.edu.vn](mailto:hiendh@uit.edu.vn)
  - Nhớ thêm mã lớp “**NT204.XXX.YYYY**” trên tiêu đề email.
- Gặp trực tiếp
  - Gửi email với GV để thống nhất thời gian và địa điểm trước khi gặp trực tiếp



# Câu hỏi/thắc mắc nếu có?

Giới thiệu môn học



# IDS/IPS

## Giới thiệu

---

NT204 – IDS/IPS

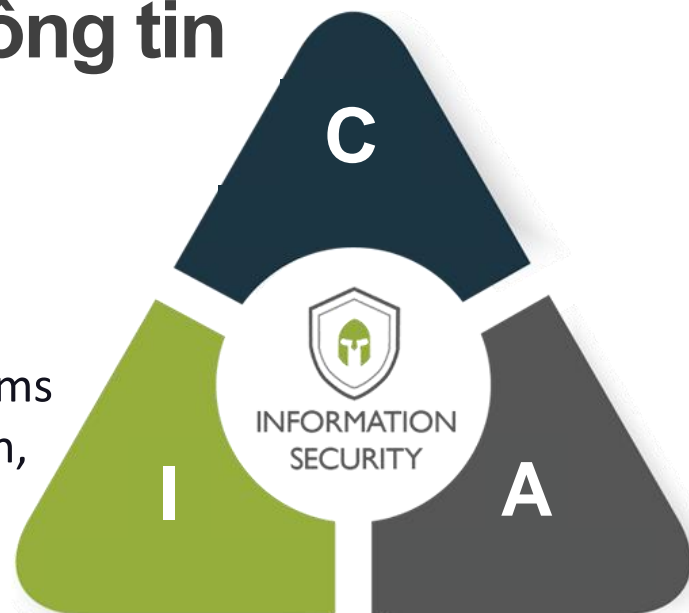


# Nhắc lại cơ bản về An toàn thông tin

An toàn thông tin là gì?

Định nghĩa **An toàn thông tin (Information Security)** (NIST):

“The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity, and availability.**”



## Bộ ba CIA?

3 “mục tiêu lớn” của an toàn thông tin:

- **Confidentiality (bảo mật)**: tránh để lộ thông tin trái phép
  - **Integrity (toàn vẹn)**: tránh để thông tin bị thay đổi trái phép
  - **Availability (sẵn sàng)**: đảm bảo những người dùng hợp lệ luôn có thể truy cập đến thông tin và hệ thống
- Mục tiêu về thông tin → kiểm soát dựa trên thông tin
- mục tiêu về hệ thống – không thể chỉ xem xét thông tin

<sup>1</sup> <https://csrc.nist.gov/glossary/term/information-security>



# Intrusions là gì? Xâm nhập là gì?

## Khái niệm



**"Intrusion** is the act of thrusting in, or of entering into a place or state without invitation, right, or welcome"

## NIST<sup>1</sup> định nghĩa:

- ***"intrusion"*** - ***xâm nhập*** là một hành vi cố gắng xâm phạm CIA, hoặc qua mặt cơ chế bảo mật của một máy tính hoặc mạng máy tính.
- Có thể có nhiều nguyên nhân:
  - malware (ví dụ, worms, spyware),
  - kẻ tấn công truy cập trái phép vào hệ thống qua mạng Internet
  - người dùng hợp lệ của hệ thống lợi dụng quyền hạn hoặc cố chiếm thêm quyền không được phép

[1] [https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps?pub\\_id=50951](https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps?pub_id=50951)

# Các tấn công mạng – intrusion phổ biến

Ôn lại một số tấn công...

## Ví dụ một số tấn công mạng

- Truy cập trái phép vào tài nguyên nào đó
  - Tiết lộ, thay đổi hoặc phá huỷ tài nguyên
- Distributed Denial of Service (DDoS) Attacks (ví dụ: Mirai botnet)
- Malware (Virus, worms, trojan, ransomware, spyware) (Ví dụ: WannaCry)
- Theo dõi và bắt lưu lượng mạng
  - User IDs, passwords, và các thông tin khác có thể bị đánh cắp qua Internet
- Khai thác các lỗ hổng phần mềm (ví dụ: buffer overflow)
- Giả dạng người dùng hợp lệ hoặc hệ thống đầu cuối
- Tấn công Web (SQLi, XSS, CSRF,...)
- DNS Attack



# Dấu hiệu chung của intrusion – xâm nhập

## Tổng quan

- Log ngắn và không đầy đủ
- Hiệu suất hệ thống thấp bất thường
- Các tiến trình bất thường
- Hệ thống bị crash hoặc reboot
- Hiện thị hình ảnh hoặc đoạn tin nhắn bất thường
- ...

Xâm nhập hệ thống	Xâm nhập mạng
<ul style="list-style-type: none"><li>▪ Xuất hiện <b>các file</b> hoặc <b>chương trình lạ</b></li><li>▪ Các <b>quyền truy cập</b> file bị thay đổi</li><li>▪ Kích thước file bị <b>thay đổi bất thường</b></li><li>▪ Những <b>tên file lạ</b> trong các <b>thư mục</b></li><li>▪ <b>Thiếu</b> file</li></ul>	<ul style="list-style-type: none"><li>▪ <b>Thăm dò</b> liên tục các service trên các máy tính</li><li>▪ Kết nối từ các <b>vị trí bất thường</b></li><li>▪ Cố gắng <b>đăng nhập liên tục</b> từ host ở xa</li><li>▪ <b>Dữ liệu bất thường</b> trong các file log, dấu hiệu của DoS hoặc hướng tới crash dịch vụ</li></ul>

Nguồn: CEHv9



# Intrusion Detection and Prevention

## Khái niệm

- **“intrusion detection” – phát hiện xâm nhập** là quy trình theo dõi các sự kiện diễn ra trong một hệ thống máy tính hoặc mạng máy tính và phân tích để nhận biết các dấu hiệu của sự bất thường (hành vi xâm nhập - intrusion).
- **“Intrusion Detection System” (IDS) – hệ thống phát hiện xâm nhập** là hệ thống phần mềm hoặc phần cứng tự động thực hiện quy trình phát hiện xâm nhập.
- **“Intrusion Prevention System” (IPS) – hệ thống ngăn chặn xâm nhập** là hệ thống **có tất cả chức năng của IDS, và** có thể **dừng** sự xâm nhập.

***Intrusion detection and prevention systems (IDPS) = IDS + IPS***

[1] [https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps?pub\\_id=50951](https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps?pub_id=50951)

# Sử dụng IDPS

## Tổng quan

- **IDPS** thường tập trung **xác định các sự cố có thể xảy ra và hỗ trợ ứng phó với sự cố**

*Ví dụ: phát hiện khi có attacker đã chiếm thành công một hệ thống bằng cách **khai thác một lỗ hổng** trên hệ thống đó*

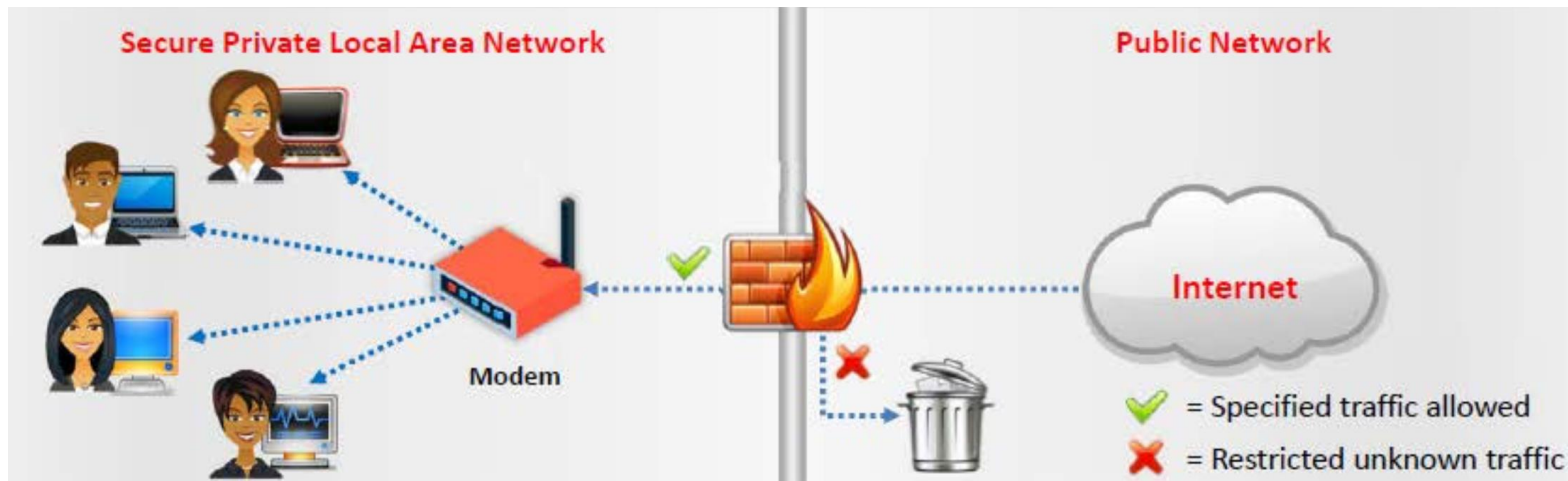
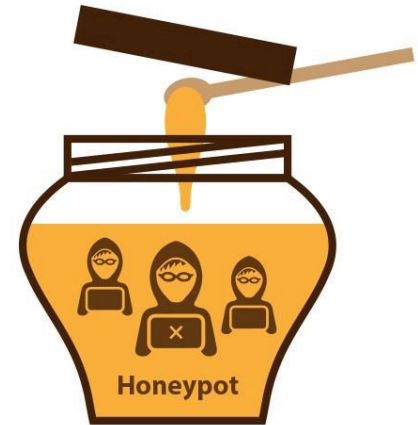
- **Ghi log** các thông tin có thể được attacker sử dụng
- **Nhận biết** các hành vi vi phạm chính sách bảo mật
- **Theo dõi** việc truyền file và xác định các file đáng ngờ
- **Xác định, chặn các hoạt động do thám**, vốn có thể là dấu hiệu sắp có tấn công (cảnh báo sớm) và thông báo cho quản trị viên
- **Xác định các vấn đề trong chính sách bảo mật**
- **Tài liệu hoá các mối đe dọa hiện có đối với 1 tổ chức**
- **Răn đe các cá nhân vi phạm chính sách bảo mật**



# Các cơ chế bảo mật Internet đã có

## Tổng quan

- Firewall – Tường lửa
- Honeypot
- Phần mềm Antivirus

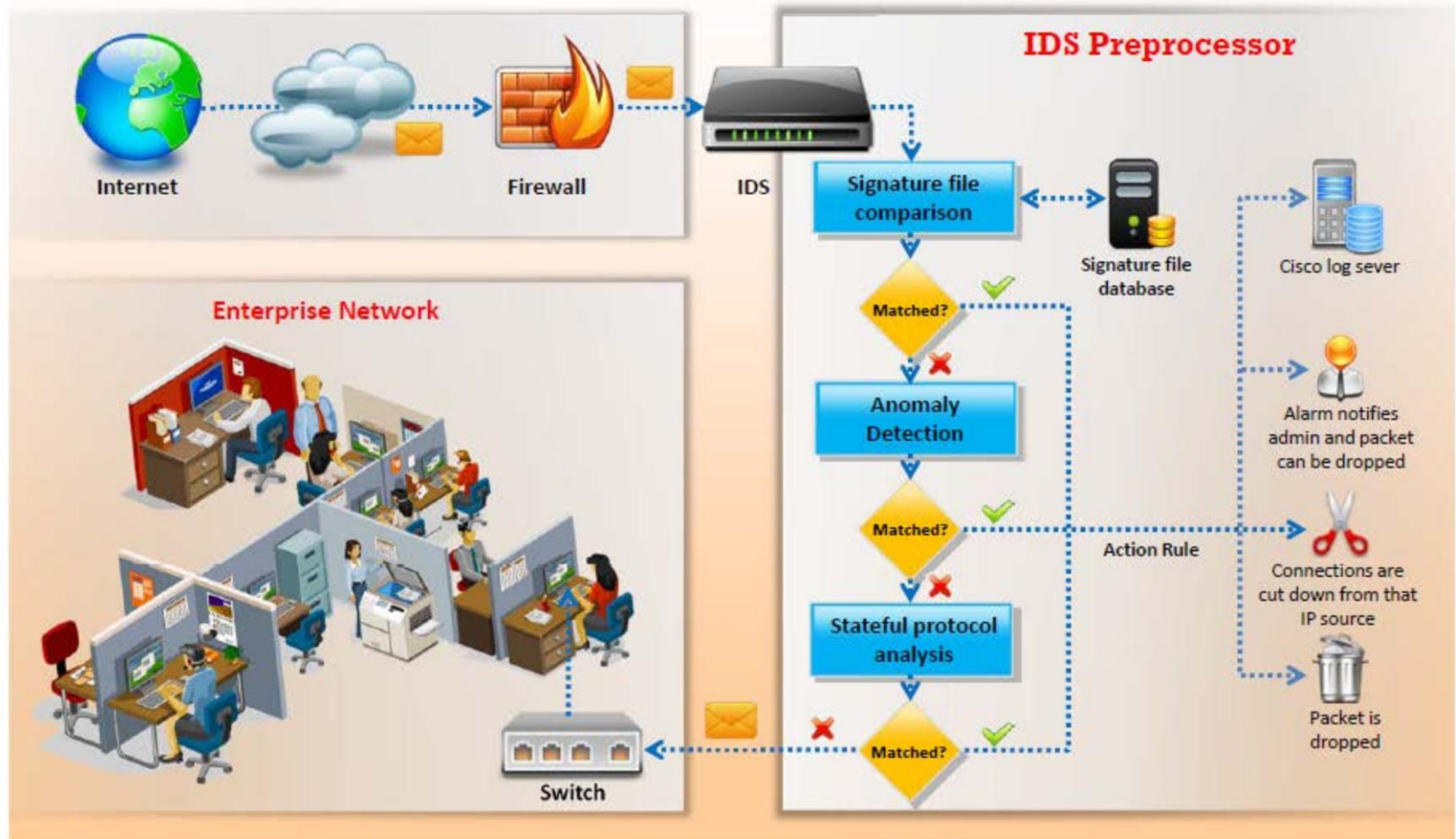


Source: CEHv9



# Cách IDS hoạt động?

## Tổng quan



Source: CEHv9





# Cách IPS ngăn chặn xâm nhập?

## Tổng quan

### 1. IPS dừng hoạt động tấn công

- ☐ Ngắt kết nối (mạng) hoặc phiên làm việc đang bị sử dụng để tấn công
- ☐ Chặn truy cập vào mục tiêu (hoặc các máy có khả năng là mục tiêu) từ tài khoản người dùng, địa chỉ IP hoặc các yếu tố tấn công khác
- ☐ Chặn tất cả các truy cập đến host, dịch vụ, ứng dụng hoặc các tài nguyên khác là mục tiêu

### 2. IPS thay đổi môi trường bảo mật

- ☐ Tái cấu hình một thiết bị mạng (ví dụ tường lửa, router, switch) để chặn truy cập từ attacker hoặc truy cập đến mục tiêu
- ☐ Vá các lỗ hổng đang có trên host

### 3. IPS thay đổi nội dung của hoạt động tấn công

- ☐ Loại bỏ hoặc thay thế những phần độc hại của tấn công để nó thành bình thường
- ☐ Hoạt động như proxy và *bình thường hoá* các yêu cầu được gửi đến (đóng gói lại payloads của yêu cầu, bỏ các thông tin header...)



# IDPS có phải lúc nào cũng phát hiện đúng?

Tổng quan

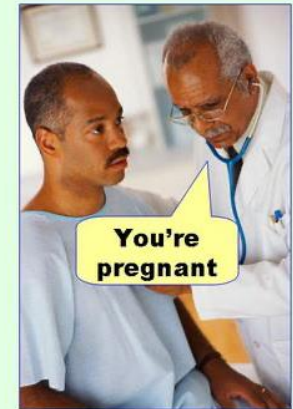
**Không!**

- ❑ **False positive – dương tính giả:** khi IDPS xác định nhầm hoạt động bình thường là hoạt động đáng ngờ
- ❑ **False negative – âm tính giả:** khi IDPS không thể xác định 1 hoạt động là đáng ngờ

➔ Mục tiêu: **Tuỳ chỉnh** IDPS để giảm tỉ lệ thông báo false (*giảm FP và FN*)

**Thực tế:** Giảm 1 tỷ lệ sẽ làm tăng tỷ lệ còn lại  
*Vậy chúng ta cần làm gì?*

**Type I error**  
(false positive)



**Type II error**  
(false negative)



# IDPS: có thể và không thể làm gì?

## Tổng quan

### ○ IDS có thể làm gì?

- IDPS có thể liên tục theo dõi các gói tin trong mạng, hiểu ở dạng nhị phân, và cảnh báo nếu xảy ra bất thường khớp với signature đã biết
- IDPS tạo ra lượng lớn dữ liệu dù được điều chỉnh tốt như thế nào

*Một IDS mới giống như 1 đứa bé, cần chăm sóc và nuôi dưỡng để trưởng thành khỏe mạnh và hiệu quả*

- Hỗ trợ các cơ chế phòng thủ mạng khác, hợp tác để hiện thực chiến lược **phòng thủ theo chiều sâu (defense-in-depth)**

### ○ IDS không thể làm gì?

- Không có IDS nào có thể thay thế sự cần thiết của đội ngũ nhân viên am hiểu về an toàn thông tin
- Không có IDS nào có thể bắt tất cả các tấn công xảy ra, hoặc chặn người khác cố gắng tấn công chúng ta



# Một vài từ khoá

Cần nhớ

- Intrusion (xâm nhập), Incident (sự cố); exploit (khai thác), vulnerability (lỗ hổng)
- Intrusion detection (phát hiện xâm nhập), Intrusion prevention (ngăn chặn xâm nhập), IDS, IPS
- False positive, False negative
- Tùy chỉnh (tuning) IDPS



# Thảo luận

Xem lại...

1. IDPS có quan trọng không?
2. Khác biệt giữa IDS và IPS?
3. Giả sử đã có 1 firewall, vậy có cần thêm IDPS? Firewall có thể hoạt động như IDPS không?

## Tuần sau:

1. Có bao nhiêu loại IDPS?  
(Tài liệu: paper “IDPS Taxonomy: traditional and state-of-the-art”)
2. IDPS có thể được đặt ở đâu trong mạng?
3. IDPS hoạt động như thế nào?



# Chuẩn bị cho tuần sau...

Looking ahead

- Hôm nay: **Giới thiệu môn học**
- Tuần sau: **Tổng quan về IDPS**
  - Nên sớm lập nhóm đồ án tối đa 4 sinh viên (có thể đăng ký tuần sau)
  - **Đọc thêm** (bài tập về nhà):
    1. Xem lại nội dung TCP/IP attack của môn NT101 – An toàn mạng máy tính
    2. G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, “**A comprehensive survey on network anomaly detection**,” *Telecommunication Systems*, vol. 70, no. 3, pp. 447–489, 2019 - <https://rdcu.be/2WNT> (Phần 1 - 4)
    3. K. Scarfone and M. Peter, **Guide to Intrusion Detection and Prevention Systems (IDPS)**. NIST, 2007. - <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> (Chương 2, 3)





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

---

