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

Tổng quan IDPS

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

GV: Đỗ Hoàng Hiển

hiendh@uit.edu.vn

Nội dung hôm nay

Tổng quan IDPS

Hôm nay:

1. **Các khái niệm IDPS**
2. Phân loại IDPS
3. Các công nghệ IDPS
   - Thành phần và kiến trúc
   - Các khả năng bảo mật
   - Quản lý

Tài liệu:

1. 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 (Section 1 - **4**)
2. 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 (Chapter 2, 3)

Nhắc lại

- **Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập** (IDPS) chủ yếu tập trung vào *xác định các sự cố có thể xảy ra, ghi nhận các thông tin liên quan, cố gắng ngăn chặn và báo cáo cho các quản trị viên bảo mật.*
  - **Mục tiêu:** đảm bảo an toàn cho mạng hoặc hệ thống máy tính theo **bộ ba CIA**.

- **Thảo luận**
  1. **Điểm khác biệt giữa IDS và IPS?**
  2. **Mô tả ít nhất 3 dạng tấn công và dấu hiệu để nhận biết chúng?**
  3. **Có bao nhiêu loại IDPS?** (dựa trên nguồn dữ liệu và kỹ thuật phát hiện tấn công)
  4. **Có thể đặt IDPS ở đâu trong một mạng? Nó có thể thay thế các hệ thống phòng thủ khác?**

Nội dung hôm nay

Tổng quan IDPS

Hôm nay:

1. Các khái niệm IDPS
2. **Phân loại IDPS**
3. Các công nghệ IDPS
   - Thành phần và kiến trúc
   - Các khả năng bảo mật
   - Quản lý

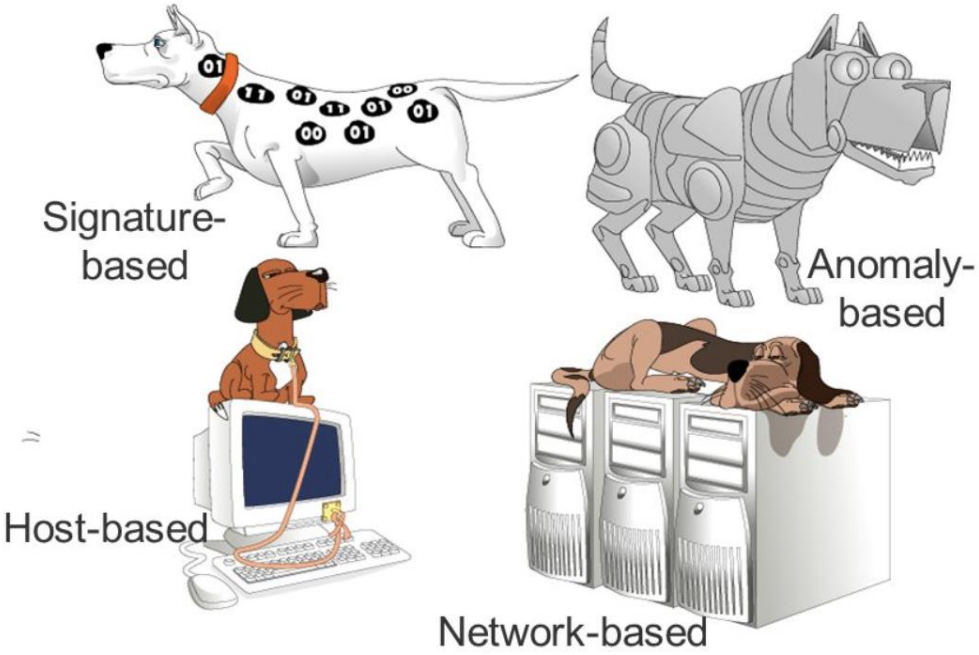
Tài liệu:

1. 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 (Section 1 - **4**)
2. 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 (Chapter 2, 3)

Phân loại IDPS dựa trên các tiêu chí khác nhau

Các dạng IDPS

- Dựa trên **Các kỹ thuật phát hiện tấn công**
  - Signature-based
  - Anomaly-based
  - Specification-based
  - Hybrid (lai)
- Dựa trên **Nguồn dữ liệu**
  - Network-based
  - Host-based
  - Hybrid (lai)



[1] 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, doi: 10.1007/s11235-018-0475-8.

Signature-Based Detection

Phân loại dựa trên Kỹ thuật phát hiện

- **Signature là gì?**

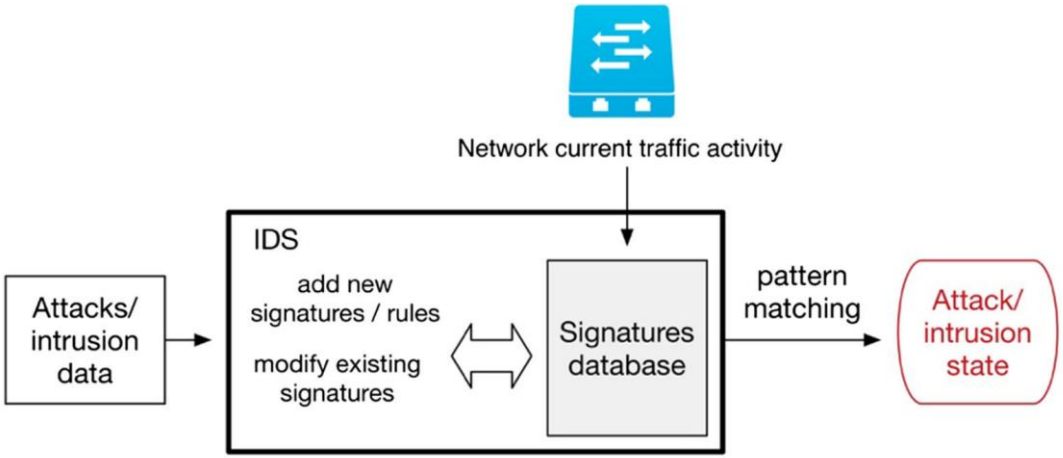
  signature là một mẫu tương ứng với một nguy cơ tấn công (cơ sở dữ liệu về *các tấn công đã biết trước*)

- ***Kỹ thuật phát hiện Signature-based*** *(hay còn gọi knowledge-based)* là một quá trình so sánh các signature với các sự kiện quan sát được để xác định các sự cố có thể có.

- Ví dụ:
  - Một kết nối telnet với username là **root** là dấu hiệu vi phạm chính sách bảo mật của 1 tổ chức.
  - Một email với tiêu đề **"Free pictures!"** và có tên file đính kèm **freepics.exe** là đặc điểm của một malware đã biết.

Signature-Based Detection (tt)

Phân loại dựa trên Kỹ thuật phát hiện



- **Ưu điểm:** Độ chính xác cao khi phát hiện các tấn công đã biết, tỉ lệ cảnh báo sai thấp.
- **Nhược điểm:**
  - Không thể phát hiện các hành vi bất thường chưa biết trước hoặc các biến đổi nhỏ trong những tấn công đã biết.

  → *Yêu cầu phải cập nhật liên tục cơ sở dữ liệu signature*

  - Việc triển khai và cập nhật signature khó và tốn thời gian.

Anomaly-Based Detection

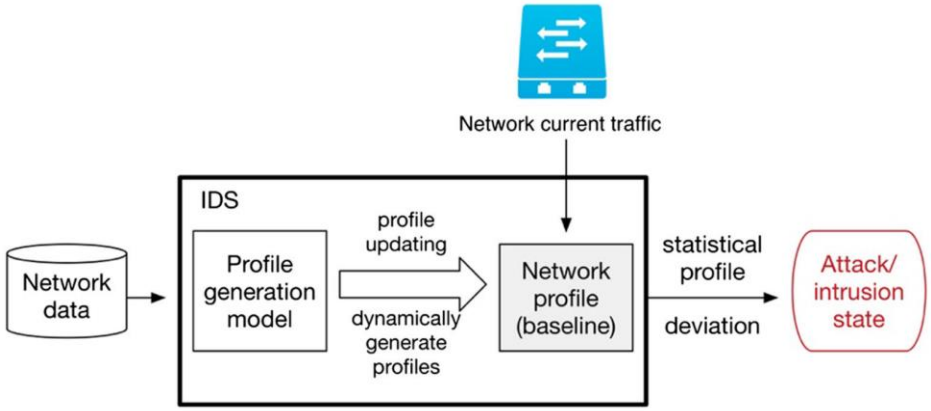
Phân loại dựa trên Kỹ thuật phát hiện

- ***Kỹ thuật phát hiện Anomaly-based*** *(hoặc profile-based)* hoạt động dựa trên việc:
  - Tạo ra một *profile cơ sở* đại diện cho các hành vi bình thường/dự kiến trong mạng.
  - Dựa trên đó, bất kỳ hoạt động mạng đang xem xét nào có sai khác so với profile này đều bị xem là bất thường.
- ***Profiles*** đại diện cho hoạt động mạng bình thường hầu hết được tạo ra thông qua phân tích lịch sử lưu lượng mạng (qua các hàm thống kê, **máy học**, clustering, fuzzy logic, heuristics…)
  - Ví dụ: Hoạt động web thường chiếm khoảng 13% băng thông mạng tại cổng Internet trong giờ hành chính của 1 doanh nghiệp.

Anomaly-Based Detection (tt)

Phân loại dựa trên Kỹ thuật phát hiện

- **Ưu điểm:**
  - Phát hiện được cả các hành vi bất thường đã biết và chưa biết, không cần phải có hiểu biết trước.
  - Phát hiện được các tấn công mới (về sau có thể sử dụng trên các signature-based IDS).



- **Nhược điểm:**
  - Tỷ lệ false positives cao (phát hiện nhầm hành vi bình thường là tấn công).
  - Ít hiệu quả quả trong các môi trường mạng động, thay đổi nhiều.
  - Yêu cầu thời gian và tài nguyên để xây dựng được profile đại diện cho mạng.

Specification-based

Phân loại dựa trên Kỹ thuật phát hiện

- ***Kỹ thuật phát hiện Specification-based*** *thu thập các hoạt động chính xác của một chương trình hoặc giao thức và theo dõi hoạt động của nó dựa trên các ràng buộc.*
  - Sử dụng mô hình giao thức chủ yếu dựa trên các chuẩn giao thức từ các nhà sản xuất phần mềm và tiêu chuẩn (IEFT, RFC)
  - Ví dụ: Thực hiện nhiều câu lệnh (command) khi ở trạng thái chưa chứng thực trong FTP thường bị xem là bất thường.
- **Ưu điểm:**
  - Xác định được các chuỗi lệnh bất thường, kiểm tra được tính hợp lý của từng câu lệnh.
  - Tỷ lệ false positive thấp.
- **Nhược điểm**:
  - Khó, thậm chí không thể phát triển các mô hình giao thức chính xác hoàn toàn.
  - Phức tạp, tốn tài nguyên và thời gian

Hybrid

Phân loại dựa trên Kỹ thuật phát hiện

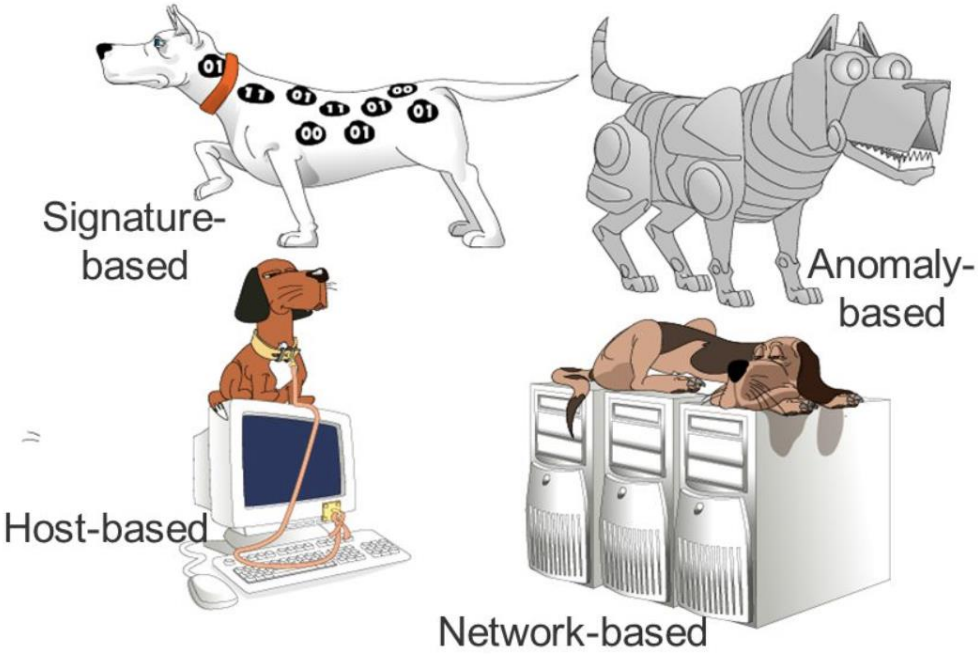
- ***Hybrid IDSs,*** *hay còn gọi Compound Detection,* kết hợp các kỹ thuật phát hiện dựa trên signature, anomaly và specification.

- **Ưu điểm:**
  - Đối phó được với các thay đổi tinh vi trong tấn công
  - Tích hợp được lợi ích của cả 3 kỹ thuật trước
  - Khắc phục được nhiều nhược điểm
- **Nhược điểm**:
  - Bị giới hạn phạm vi vào hoạt động của một chương trình giao thức
  - Cần tích hợp sao cho 3 kỹ thuật riêng biệt có thể cùng tương tác và hoạt động trong cùng một hệ thống.

Phân loại IDPS dựa trên các tiêu chí khác nhau

Các dạng IDPS

- Dựa trên **Các kỹ thuật phát hiện tấn công**
  - Signature-based
  - Anomaly-based
  - Specification-based
  - Hybrid (lai)
- Dựa trên **Nguồn dữ liệu**
  - Network-based
  - Host-based
  - Hybrid (lai)

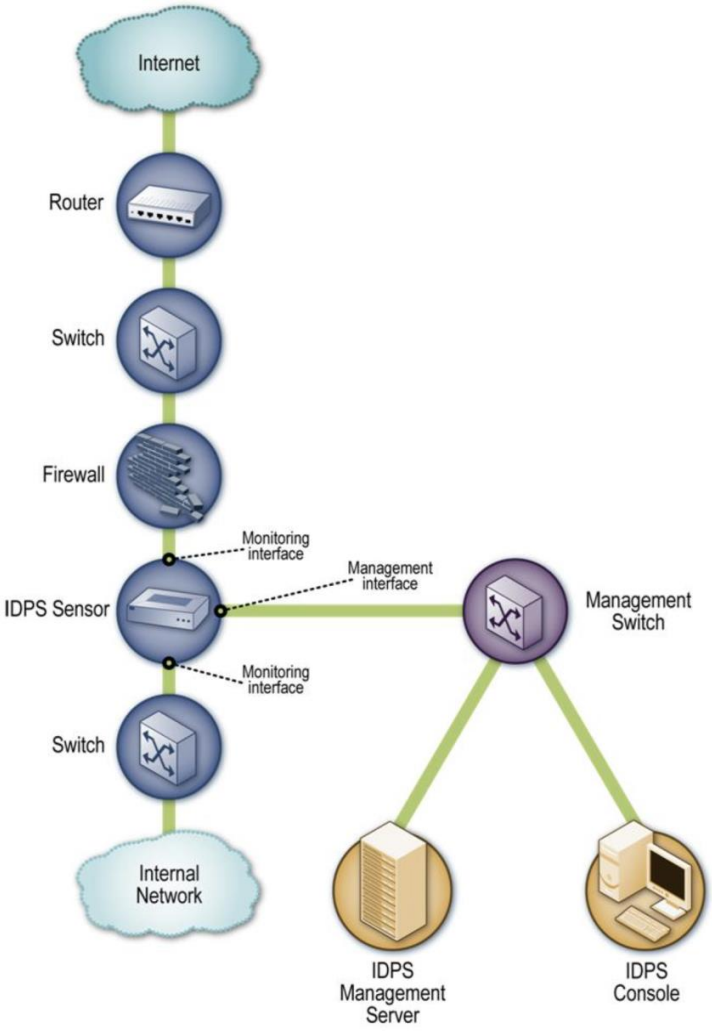


[1] G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, “A comprehensive survey on network anomaly detection,” *Telecommunication Systems*, vol. 70, no. 3, pp. 447–489, 2019, doi: 10.1007/s11235-018-0475-8.

Network-based IDPS (NIDPS)

Phân loại dựa trên Nguồn dữ liệu và vị trí

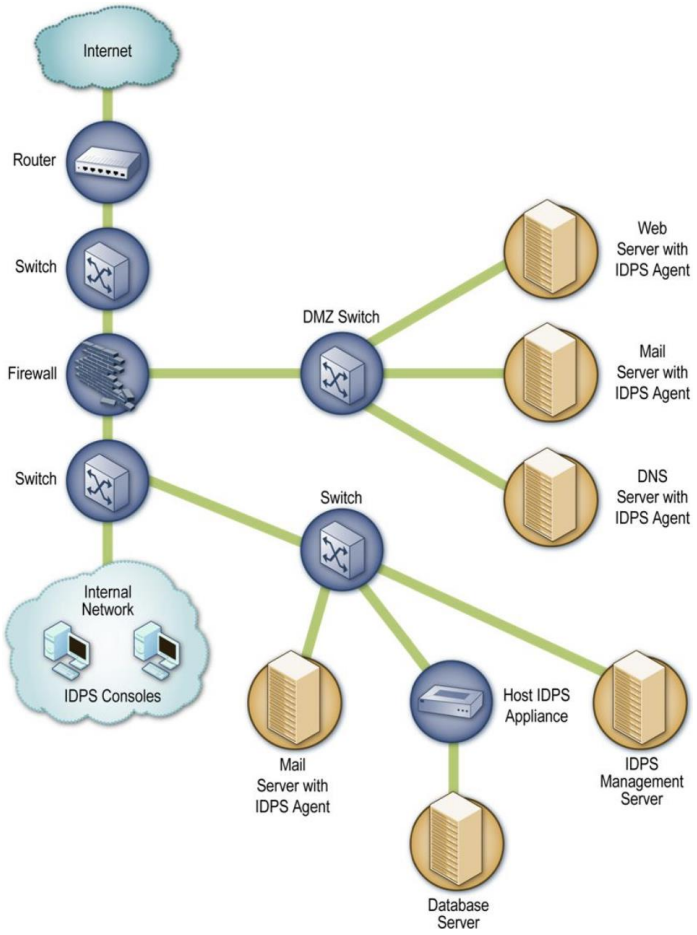
- ***Network-based IDPS (NIDPS)*** theo dõi lưu lượng mạng cho *một phần của mạng (network segment) hoặc các thiết bị*, phân tích các hoạt động mạng và các giao thức, ứng dụng để xác định các hành vi bất thường.
  - Thường triển khai ở **biên mạng**, *như gần tường lửa hoặc router biên, server VPN, server remote access và mạng không dây*.
  - *Gồm nhiều **sensor** đặt ở nhiều điểm khác nhau trong mạng để theo dõi lưu lượng mạng.*



Host-based IDPS (HIDPS)

Phân loại dựa trên Nguồn dữ liệu và vị trí

- ***Host-based IDPS (HIDPS),*** theo dõi các đặc điểm của một host riêng lẻ và các sự kiện xảy ra trong host đó để phát hiện hoạt động bất thường.
  - *Theo dõi: lưu lượng mạng của host, log hệ thống, các tiến trình đang chạy, các hoạt động ứng dụng, truy cập và thay đổi file, thay đổi trong cấu hình hệ thống hay ứng dụng,…*
  - Được triển khai trên **host quan trọng** *(các server có thể truy cập từ bên ngoài, các server chứa thông tin quan trọng)*.



Hybrid IDPS

Phân loại dựa trên Nguồn dữ liệu và vị trí

- ***Hybrid IDPS*** được phát triển để hướng đến **xem xét tất cả dữ liệu** từ các sự kiện trên host và sự kiện trong các phần mạng, **kết hợp chức năng** của cả network và host-based IDPSs
  - Tích hợp các ưu điểm của cả 2 kỹ thuật trên.
  - Cần tích hợp sao cho 2 kỹ thuật riêng biệt có thể cùng tương tác và hoạt động trong cùng một hệ thống.

Nội dung hôm nay

Tổng quan IDPS

Hôm nay:

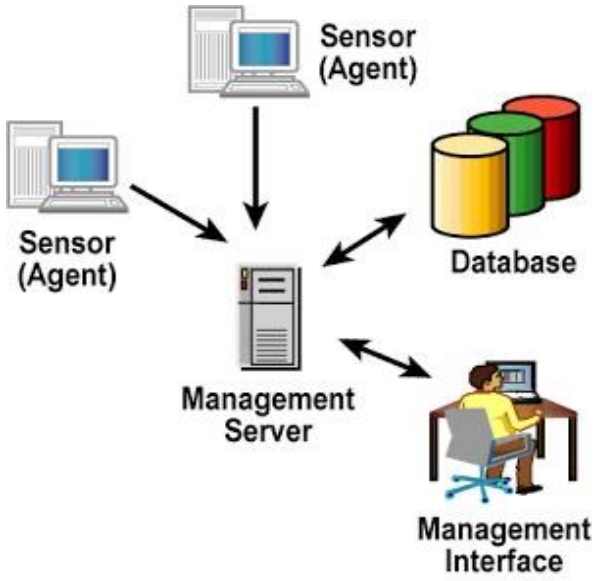
1. Các khái niệm IDPS
2. Phân loại IDPS
3. **Các công nghệ IDPS**
   - Thành phần và kiến trúc
   - Các khả năng bảo mật
   - Quản lý

Tài liệu:

1. 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 (Section 1 - **4**)
2. 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 (Chapter 2, 3)

IDPS: Các thành phần chính

Các công nghệ IDPS



- **Sensor hoặc Agent:** theo dõi và phân tích các hoạt động
  - **Sensor:** Network-based IDPS
  - **Agent:** Host-based IDPS
- **Server quản lý:** thiết bị trung tâm nhận các thông tin từ các sensor hoặc agent để quản lý.
- **Server cơ sở dữ liệu:** nơi lưu trữ các thông tin sự kiện theo dõi được bởi các sensor hay agent và server quản lý (o*ptional)*
- **Consoles:** chương trình cung cấp giao diện tương tác với IDPS cho người dùng hoặc quản trị viên (GUI or CLI)

IDPS: Kiến trúc

Các công nghệ IDPS

- **Các thành phần của IDPS có thể được kết nối với nhau thông qua**
  - Các mạng chuẩn (standard networks) của tổ chức, *hoặc*
  - Một mạng tách biệt được thiết kế riêng cho việc quản lý an toàn thông tin - ***mạng quản lý***

Mạng quản lý

- **Ưu điểm:**
  - **Độc lập** đối với mạng sản xuất của doanh nghiệp
  - **Che giấu** được sự tồn tại và dấu hiệu của IDPS với attacker
  - **Bảo vệ** IDPS khỏi tấn công và đảm bảo IDPS có đủ băng thông để hoạt động trong điều kiện bất lợi (do tấn công)
- **Nhược điểm:**
  - Cần thêm chi phí cho hạ tầng mạng và các phần cứng khác
  - **Bất tiện** cho người dùng và quản trị viên IDPS

Cách khác?

Mạng quản lý ảo với VLAN

- ***Nhưng*** *VLAN không được bảo vệ tốt như mạng quản lý*

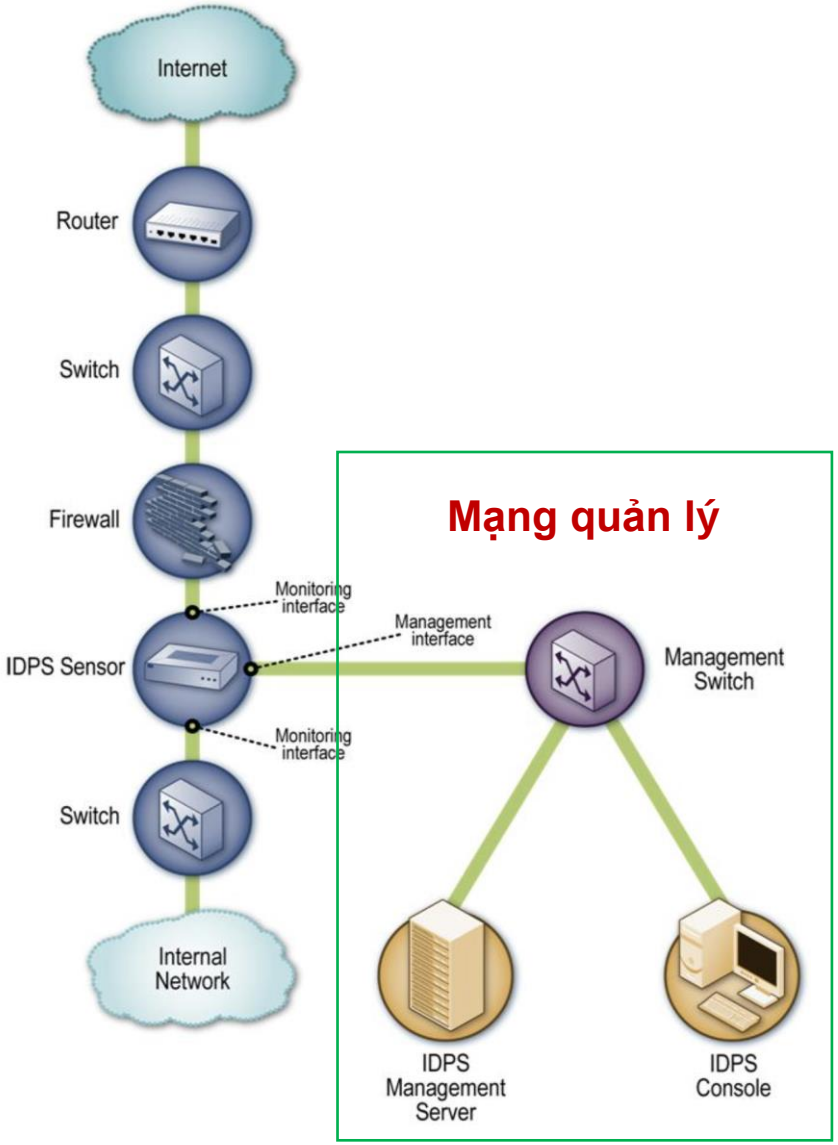
IDPS: Kiến trúc (tt)

Các công nghệ IDPS

- **Ví dụ:**

Kiến trúc *Network-based IDPS*

- *Các server quản lý, server cơ sở dữ liệu và console chỉ được gắn với mạng quản lý.*
- *Các sensor không thể gửi bất kỳ lưu lượng nào giữa **interface quản lý** của chúng với bất kỳ interface mạng nào khác của nó.*



IDPS: Các khả năng bảo mật

Các công nghệ IDPS

1. Thu thập thông tin

- Thu thập thông tin trên host hoặc mạng từ các hoạt động quan sát được
  Ví dụ: OS, các host, các ứng dụng được dùng, xác định các đặc điểm chung của mạng,…

2. Ghi log

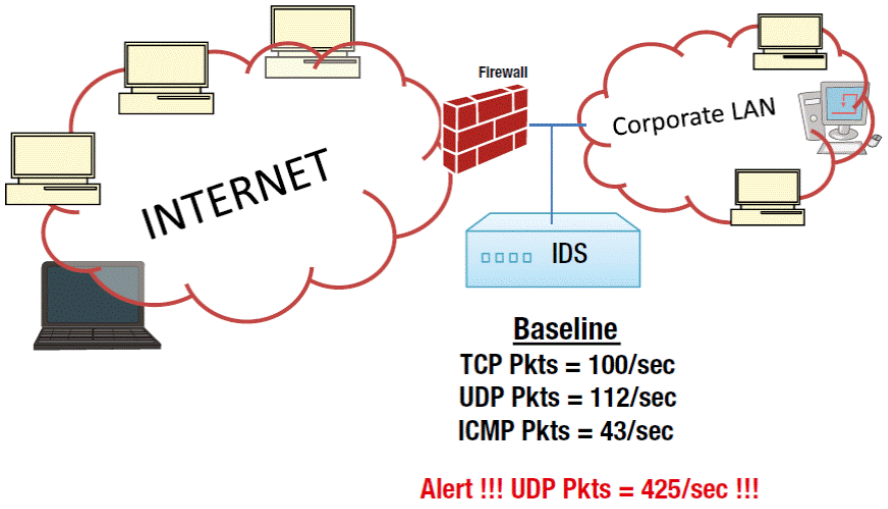
- Ghi log các dữ liệu liên quan đến sự kiện phát hiện được
- Ghi log các dữ liệu có thể được dùng để kiểm tra **tính hợp lệ** của cảnh báo, điều tra các sự số và liên kết các sự kiện giữa IDPS và các nguồn log khác.
- **Các trường dữ liệu phổ biến:** *thời gian xảy ra sự kiện, loại sự kiện, mức độ quan trọng* (ví dụ độ ưu tiên, mức độ nghiêm trọng, tác động, độ tin cậy)*, hành động ngăn chặn đã thực hiện (*nếu có*), gói tin bắt được* (NIDS)*, user ID* (HIDS)
- Thông thường, log nên được lưu trữ ở cả **nội bộ** và **tập trung** để đảm bảo **tính toàn vẹn** và **sẵn sàng** của dữ liệu.

IDPS: Các khả năng bảo mật (tt)

Các công nghệ IDPS

3. Phát hiện:

- **Ngưỡng (thresholds):** là 1 giá trị thiết lập giới hạn giữa hành vi bình thường và bất thường, xác định mức độ tối đa có thể chấp nhận được (là bình thường).
  - Ví dụ: ***x*** lần đăng nhập lỗi trong 60 giây, hoặc ***y*** ký tự cho độ dài của tên file
  - Thường được dùng cho ***kỹ thuật phát hiện anomaly-based*** và ***phân tích các stateful protocol.***



IDPS: Các khả năng bảo mật (tt)

Các công nghệ IDPS

3. Phát hiện (tt)

- **Blacklists và Whitelists**
  - **Blacklists** *(hot lists)*: là một danh sách các thực thể rời rạc *(có thể là hosts, port TCP hay UDP, ICMP types và codes, ứng dụng, usernames, URLs, tên file, hay phần mở rộng file)* đã được xác định trước đó là **có liên quan đến hoạt động độc hại**, được dùng để nhận dạng và chặn các hoạt động có nguy cơ cao là **có hại**, và cũng dùng để gán độ ưu tiên cho hơn cho các cảnh báo có liên quan đến blacklist.
  - **Whitelist**: là một danh sách các thực thể rời rạc đã được biết là **bình thường**, được sử dụng nhằm giảm hoặc loại bỏ các trường hợp false positive (dương tính giả) bao gồm các hoạt động bình thường từ các host đáng tin cậy.
  - thường sử dụng cho ***kỹ thuật phát hiện signature-based*** và ***phân tích các stateful protocol***

IDPS: Các khả năng bảo mật (tt)

Các công nghệ IDPS

3. Phát hiện (tt)

- **Thiết lập cảnh báo**
  - Bật hoặc tắt chức năng cảnh báo
    - Ở một số công nghệ IDPS, tắt cảnh báo cũng tắt luôn khả năng phát hiện tấn công
    - Ở một số sản phẩm khác, quá trình phát hiện vẫn được thực hiện nhưng không tạo ra các thông điệp cảnh báo
  - Thiết lập giá trị mặc định cho mức độ ưu tiên và mức độ nghiêm trọng
  - Xác định những thông tin cần ghi nhận lại và các phương pháp thông báo (ví dụ email, SMS, thông báo ứng dụng) nên dùng.
  - Xác định khả năng ngăn chặn được dùng.
  - Ngưng việc cảnh báo nếu attacker tạo nhiều cảnh báo trong khoảng thời gian ngắn và tạm thời bỏ qua tất cả các lưu lượng mạng từ attacker

IDPS: Các khả năng bảo mật (tt)

Các công nghệ IDPS

3. Phát hiện (tt)

- **Xem và chỉnh sửa mã nguồn**

Một vài công nghệ IDPS (IDPS mã nguồn mở) cho phép quản trị viên xem một phần hoặc toàn bộ mã nguồn liên quan đến việc phát hiện tấn công.

- Xem mã nguồn liên quan đến phát hiện tấn công giúp xác định cụ thể cảnh báo nào sẽ được tạo, xác nhận lại các cảnh báo và xác định tỷ lệ false positive.
- Chỉnh sửa tất cả các mã nguồn liên quan đến phát hiện tấn công và viết mã nguồn mới *(ví dụ, signature mới)* là điều thiết yếu để tuỳ chỉnh khả năng phát hiện tấn công.
  - Cần kỹ năng lập trình và phát hiện tấn công
  - Quá trình tuỳ chỉnh có thể làm phát sinh một số bugs trong mã nguồn

IDPS: Các khả năng bảo mật (tt)

Các công nghệ IDPS

3. Phát hiện (tt)

Quản trị viên nên định kỳ kiểm tra lại **việc tuỳ chỉnh** để đảm bảo hệ thống vẫn hoạt động chính xác

- **Ngưỡng và các thiết lập cảnh báo** có thể cần điều chỉnh định kỳ để đáp ứng với những thay đổi trong môi trường cũng như các mối đe doạ.
- **Whitelists và blacklists** nên được kiểm tra thường xuyên và các thực thể (entry) nên được kiểm tra để đảm bảo vẫn chính xác và cần thiết.
- **Các thay đổi trong mã nguồn phát hiện tấn công** có thể cần sao chép lại mỗi khi sản phẩm được cập nhật (ví dụ: vá lỗ hổng, nâng cấp)

IDPS: Các khả năng bảo mật (tt)

Các công nghệ IDPS

4. Ngăn chặn

- IDPS thường cho phép quản trị viên cấu hình khả năng ngăn chặn **cho mỗi loại cảnh báo** mà nó đưa ra.
- Thường bao gồm **bật/tắt** khả năng ngăn chặn, cũng như chỉ định rõ **loại khả năng ngăn chặn** nào nên dùng.

IDPS: Quản lý

Các công nghệ IDPS

Hầu hết IDPS đều cung cấp khả năng quản lý tương tự nhau:

- **Triển khai**
  - Thiết kế kiến trúc
  - Kiểm tra và triển khai các thành phần
  - Bảo vệ các thành phần IDPS
- **Vận hành và bảo trì**
  - Bảo trì giải pháp đang hoạt động
  - Tải và cài đặt các bản cập nhật
- **Các khuyến nghị khi triển khai và bảo trì**

IDPS: Triển khai

Quản lý IDPS

- **Thiết kế kiến trúc –** *cần quan tâm đến:*
  - Đặt các sensor hay agent **ở đâu**?
  - Giải pháp cần có **độ tin cậy** như thế nào và dùng **các thông số** nào để đạt được độ tin cậy đó?
  - Đặt các thành phần khác của IDPS **ở đâu**?
  - Mỗi thành phần cần **số lượng bao nhiêu** để đạt mục tiêu về khả năng **sử dụng**, **dự phòng** và **cân bằng tải**?
  - IDPS cần **giao tiếp** với các hệ thống nào khác?
    - Hệ thống cung cấp dữ liệu *(vd. DMZ server, log server tập trung, e-mail servers)*
    - Hệ thống để thực hiện các phản ứng ngăn chặn*(vd., tường lửa, routers, switches)*
    - Hệ thống quản lý các thành phần IDPS *(vd. phần mềm quản lý mạng hay bản vá)*
  - **Có cần sử dụng** mạng quản lý hay không? Thiết kế như thế nào để bảo vệ IDPS?
  - Những cơ chế hay công nghệ kiểm soát bảo mật nào cần phải thay đổi để **phù hợp với** triển khai IDPS?

IDPS: Triển khai

Quản lý IDPS

- **Kiểm tra và triển khai các thành phần**
  - Nên triển khai trước trong một **môi trường thử nghiệm**, để tránh xảy ra trường hợp các sự cố khi triển khai làm gián đoạn mạng sản xuất.
  - Triển khai một IDPS có thể yêu cầu **ngưng** mạng hoặc hệ thống **trong thời gian ngắn** để cài đặt các thành phần.
  - **Các IDPS phần cứng** thường dễ triển khai hơn **các IDPS phần mềm.**
  - Sau khi triển khai, tuỳ vào loại IDPS đang triển khai, có thể cần cấu hình khả năng **phát hiện và ngăn chặn tấn công** của sản phẩm.

    Nếu không cấu hình, một số IDPS chỉ có thể phát hiện số lượng ít các tấn công cũ, dễ phát hiện.

IDPS: Triển khai

Quản lý IDPS

- **Bảo vệ các thành phần IDPS**
  - Là 1 việc **rất quan trọng** do IDPS thường là mục tiêu của attacker
  - Quản trị viên nên:
    - Tạo các tài khoản **riêng biệt** cho mỗi người dùng và quản trị viên cho IDPS, chỉ cung cấp các quyền hạn cần thiết.
    - Cấu hình tường lửa, router, và các thiết bị lọc gói tin khác để **hạn chế truy cập trực tiếp** đến các thành phần IDPS, chỉ cho phép các host thực sự cần truy cập.
    - Đảm bảo tất cả các giao tiếp trong quản lý IDPS đều được **bảo vệ,** thông qua tách biệt vật lý (ví dụ mạng quản lý) hoặc logic (ví dụ VLAN quản lý), hoặc thông qua mã hoá các giao tiếp.

IDPS: Quản lý

Các công nghệ IDPS

Vận hành và bảo trì

Hầu như tất cả IDPS đều được thiết kế để vận hành và bảo trì thông qua giao diện người dùng (GUI) còn gọi là ***console***.

- Cho phép quản trị viên cấu hình và cập nhật các sensors, server và theo dõi trạng thái của chúng *(e.g., agent failure, packet dropping).*
- Cung cấp nhiều tính năng hỗ trợ người dùng thực hiện các tác vụ định kỳ (e.g. kiểm tra cảnh báo, phân tích và bắt gói tin) với nhiều tính năng **báo cáo**.
- Một số IDPS có thể dùng **command-line interfaces** (CLI) *(quản lý thông qua SSH)*

IDPS: Quản lý

Các công nghệ IDPS

- **Bảo trì giải pháp, Tải và cài đặt bản cập nhật**
  - ✓ Theo dõi các vấn đề vận hành và bảo mật trên các thành phần IDPS.
  - ✓ Định kỳ kiểm tra IDPS có đang hoạt động chính xác không *(vd., xử lý các sự kiện, cảnh báo phù hợp khi có hoạt động đáng ngờ).*
  - ✓ Thường xuyên thực hiện đánh giá các lỗ hổng có thể có.
  - ✓ Nhận và phản hồi tương ứng với các thông báo từ nhà sản xuất về các vấn đề bảo mật đối với các thành phần IDPS *(bao gồm OS và các ứng dụng không liên quan đến IDPS).*
  - ✓ Nhận thông báo cập nhật từ nhà sản xuất IDPS, thực hiện kiểm tra và cài đặt các bản cập nhật.
    - **Cập nhật phần mềm**: sửa các bugs trong phần mềm IDPS hoặc thêm tính năng mới.
    - **Cập nhật signature**: thêm khả năng phát hiện tấn công mới hoặc điều chỉnh tấn công đã có.

  Quản trị viên nên kiểm tra bản cập nhật phần mềm và signature trước khi cài đặt, ngoại trừ các trường hợp khẩn cấp.

IDPS: Quản lý

Các công nghệ IDPS

- **Các khuyến nghị trong triển khai và bảo trì**
  - Quản trị viên **triển khai** các thành phần IDPS cần có những *kiến thức cơ bản về quản trị hệ thống, quản trị mạng và an toàn thông tin.*
  - Quản trị viên **tuỳ chỉnh** IDPS cần có *kiến thức bao quát phù hợp về an toàn thông tin và nguyên tắc hoạt động của IDPS.*
  - *Kỹ năng lập trình* cần cho việc tuỳ chỉnh mã nguồn, viết report và nhiều tác vụ khác.
- Hiểu biết về các sản phẩm IDPS cụ thể thông qua:
  - **Training từ nhà sản xuất**: *courses, seminar, webinar*
  - **Tài liệu sản phẩm**: *manual, installation guide, user's guide, administrator's guide*
  - **Hỗ trợ kỹ thuật**
  - **Các dịch vụ chuyên gia**: *consulting, write custom signatures or reports*
  - **Cộng đồng người dùng**: *mailing lists, online forum, Github, Stackoverflow*

Tóm lại

Kiến thức cần nhớ

- Phân loại IDPS

Dựa trên kỹ thuật phát hiện
- Signature-based
- Anomaly-based
- Specification-based
- Hybrid

Dựa trên nguồn dữ liệu
- Network-based
- Host-based
- Hybrid

- IDPS không thể cung cấp khả năng phát hiện chính xác hoàn toàn, đều có thể có tỷ lệ false positive và false negative. IDPS nên được sử dụng để hỗ trợ các cơ chế phòng thủ khác (tường lửa, antivirus…)
- **Các thành phần chủ yếu** trong IDPS gồm các *sensor hay agent, server quản lý, server cơ sở dữ liệu, và console*
- Hầu hết các IDPS có thể cung cấp nhiều khả năng bảo mật đa dạng: thu thập thông tin, ghi log, phát hiện tấn công *(sử dụng ngưỡng, blacklist-whitelist, hỗ trợ thiết lập cảnh báo, chỉnh sửa mã nguồn)* và ngăn chặn tấn công.
- Một khi đã lựa chọn được giải pháp IDPS, quản trị viên cần *thiết kế kiến trúc, thực hiện kiểm tra các thành phần IDPS, triển khai và bảo vệ các thành phần này*.

Tuần sau…

- Hôm nay: **Tổng quan về IDPS**

- Chuẩn bị cho tuần sau: **Network-based IDPS**
  - Tài liệu: NIST Chapter 4 và papers, tài liệu liên quan
  - Đăng ký nhóm đồ án cuối kỳ, thông báo danh sách các chủ đề.

Câu hỏi/thắc mắc nếu có???

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