Chương 8

HỆ THỐNG PHÁT HIỆN - NGĂN NGỪA XÂM NHẬP MẠNG

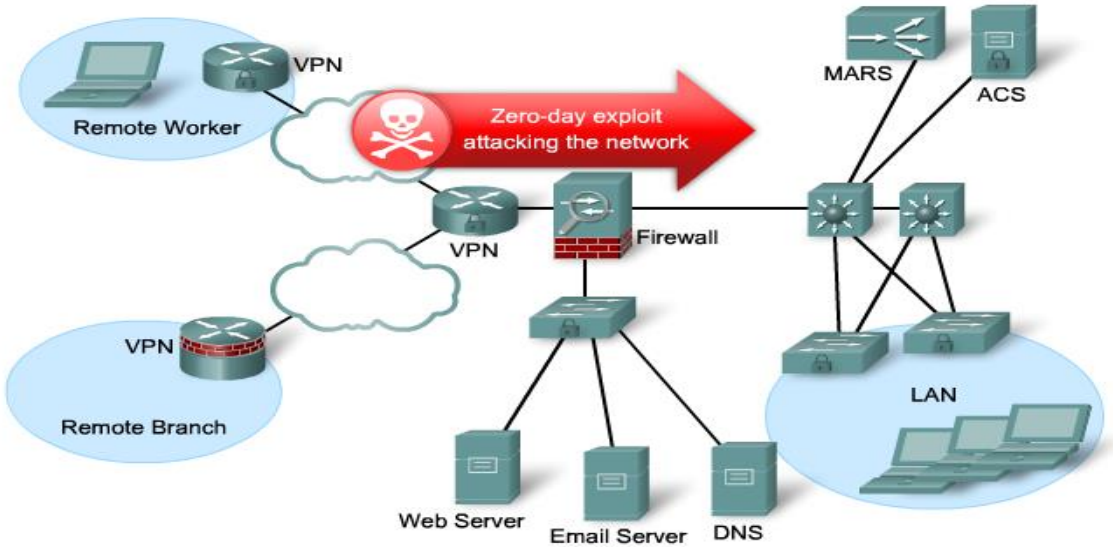
Trình bày: Bùi Minh Quân - bmquan@ctu.edu.vn

Khoa MMT&TT – Trường CNTT&TT - ĐHCT

HỆ THỐNG PHÁT HIỆN - NGĂN NGỪA XÂM NHẬP MẠNG

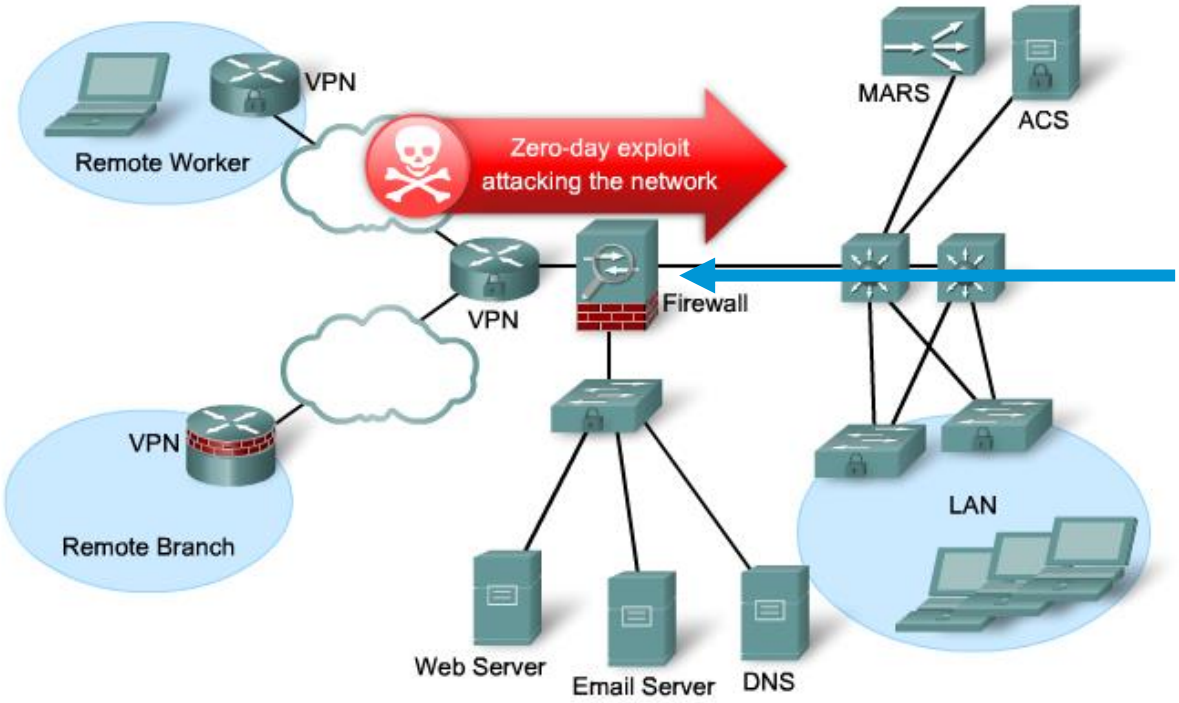
Zero-Day Exploits

- Worm và virus có thể lây lan mạng toàn cầu với tốc độ rất nhanh.
  - **Zero-day attack** (zero-day threat), là một cuộc tấn công máy tính để cố gắng khai thác lỗ hổng phần mềm.
  - **Zero-hour:** mô tả thời điểm khai thác được phát hiện.



Zero-Day Exploits

- Làm thế nào để dừng các cuộc tấn công kiểu zero-day?
  - Firewalls thì không thể làm được điều này!



Firewalls không thể dừng các cuộc tấn công kiểu malware hoặc zero-day

Bảo vệ máy tính bằng cách nào?

- Người dùng…
  - Ngồi hàng giờ để theo dõi hệ thống qua Task Manager để phát hiện các tiến trình bất thường?
  - Quan sát trong bản ghi Event Viewer tìm kiếm các sự kiện bất thường?
- Dựa vào các phần mềm chống Virus, tường lửa.

Bảo vệ mạng máy tính bằng cách nào?

- Người quản trị thường xuyên theo dõi và phân tích các logfile để ghi nhận các bất thường
- Giới hạn của cách thức phân tích logfile
  - Việc phân tích thủ công mất nhiều thời gian
  - Có cái nhìn hạn chế về các cuộc tấn công đang diễn ra
  - Tại thời điểm phân tích logfile, các cuộc tấn công vẫn liên tục diễn ra, thậm chí hệ thống đích có thể đã dừng hoạt động

Các giải pháp

- Một giải pháp tốt phải đảm bảo cho mạng phải có khả năng ***tức thì*** nhận ra và giảm thiểu các mối đe dọa từ worm và virus.
- Hai giải pháp đã phát triển:
  - Intrusion Detection Systems (IDS) ❋ First generation
  - Intrusion Prevention Systems (IPS) ❋ Second generation
- Công nghệ IDS và IPS sử dụng bộ quy tắc, các tập luật, gọi là ***signatures***, để phát hiện hoạt động xâm nhập điển hình.

Các "cảm biến" IDS và IPS

- Công nghệ IDS và IPS được phát triển như các **'bộ cảm biến'** được cài đặt trên các **thiết bị**:
  - Một router được cấu hình với phần mềm IPS (Vd: Cisco IOS IPS)
  - Một mô-đun được cài đặt vào các thiết bị như **router hay một switch**
  - Một thiết bị chuyên dụng được thiết kế để cung cấp dịch vụ IDS, IPS
  - Phần mềm chạy trên các máy tính (clients/servers)
- Lưu ý:
  - Có nhiều giải pháp khác nhau để triển khai IPS và các giải pháp này có một số khác biệt nhất định

Cách hoạt động

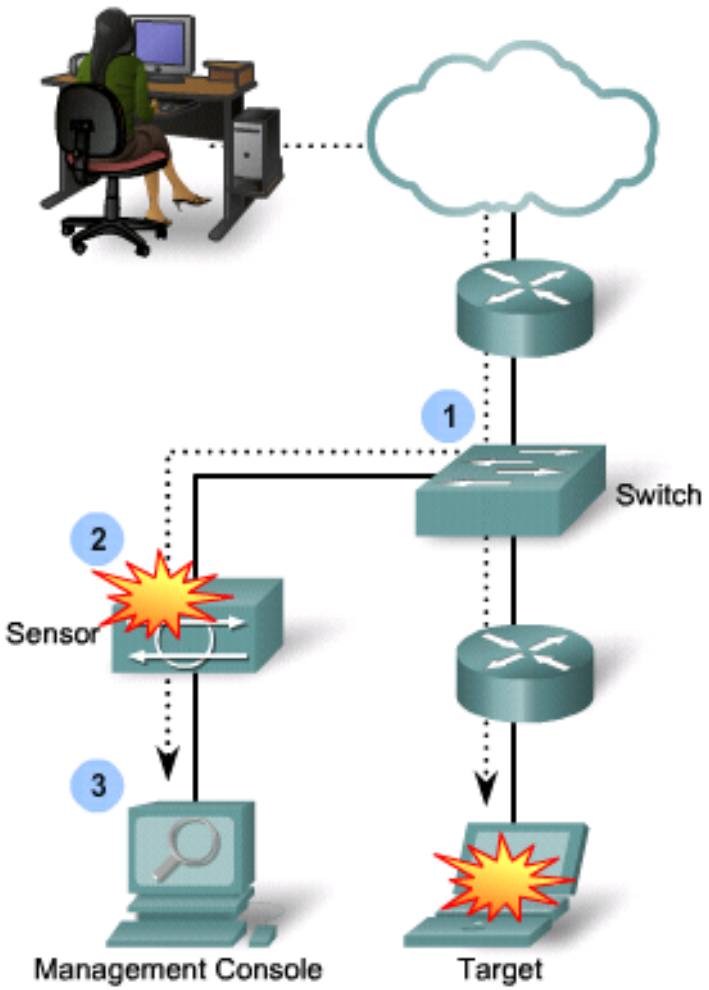
- **Thu thập và phân tích dữ liệu:** thu thập các gói tin, các luồng dữ liệu hay các hoạt động trên mạng. Nhận diện các hoạt động xâm nhập, cập nhật liên tục từ các nhà cung cấp hay được tự tạo bởi quản trị viên.
- **Phát hiện và ngăn chặn xâm nhập:** IDS chỉ phát hiện xâm nhập mạng. Nếu IPS phát hiện được một hoạt động xâm nhập, nó sẽ ngay lập tức áp dụng các biện pháp ngăn chặn để dừng lại hoạt động đó. Các biện pháp ngăn chặn có thể là: cắt kết nối, xoá gói tin, thay đổi nội dung gói tin, thay đổi cấu hình firewall hay gửi thông báo cho quản trị viên.

Cách hoạt động

- **Gửi cảnh báo:** gửi cảnh báo cho quản trị viên về các hoạt động xâm nhập qua các kênh như email, SMS, web hay máy tính. Lưu trữ các thông tin về các hoạt động xâm nhập, như thời gian, nguồn, đích, loại tấn công,… để phục vụ cho việc kiểm tra, phân tích hay điều tra.

Intrusion Detection Systems - IDS

Intrusion Detection System - IDS



Một IDS giám sát thông tin về các lưu thông **đã diễn ra** và phát ra các các cảnh báo nếu phát hiện các bất thường :

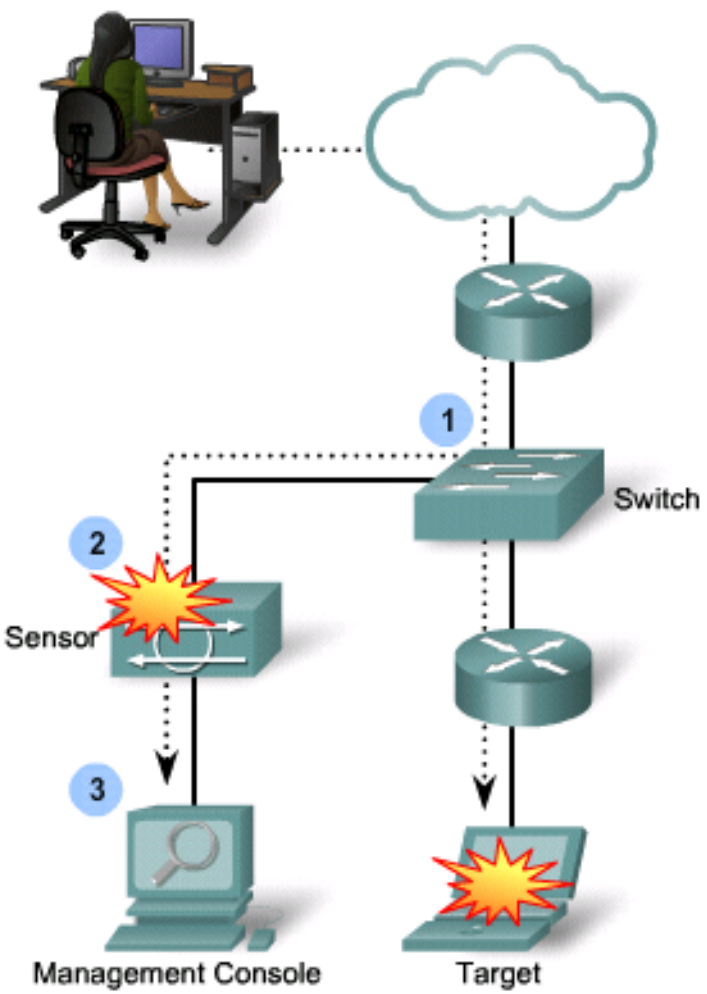
- Reconnaissance attacks (tấn công thăm dò)
- Access attacks (tấn công truy cập)
- Denial of Service attacks (tấn công từ chối dịch vụ)

Intrusion Detection System - IDS

- IDS có thể được triển khai dưới dạng:
  - Giải pháp dựa trên mạng
  - Giải pháp dựa trên máy chủ
- Ở cả hai vị trí triển khai, nó giám sát lưu lượng mạng và các hoạt động độc hại khác để xác định các cuộc xâm nhập tiềm ẩn và các mối đe dọa khác đối với mạng hoặc thiết bị được giám sát.

https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/

Intrusion Detection System - IDS



- **IDS** làm việc ở chế độ **thụ động** bởi vì nguyên lý hoạt động của IDS là phân tích dựa trên bản sao, dấu vết của các luồng lưu thông.
  - Không ảnh hưởng đến tốc độ lưu thông trên mạng.
  - Các lưu thông chứa mã độc vẫn lưu thông trên mạng ngay cả khi IDS đang hoạt động.

Intrusion Detection System - IDS

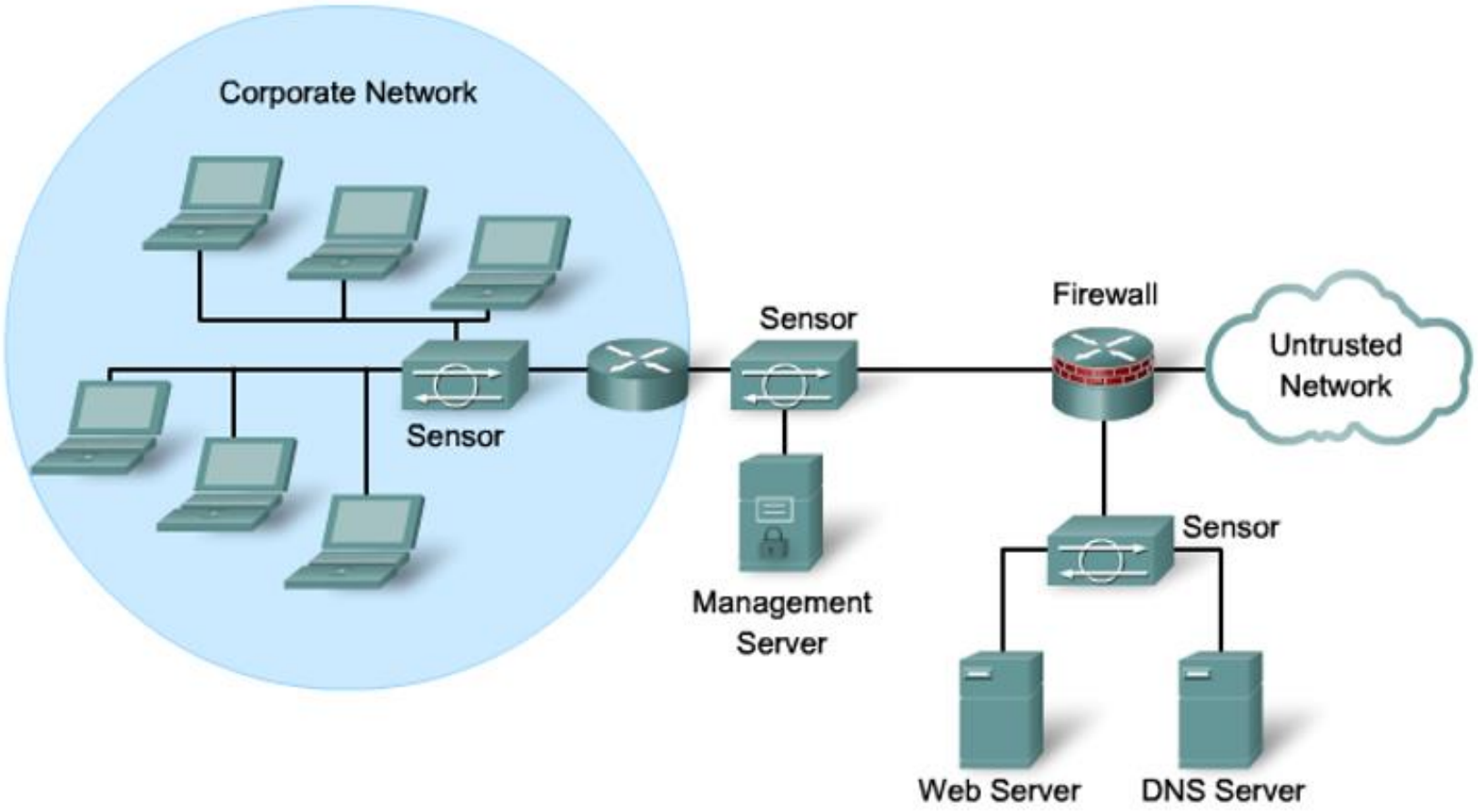
- **Phương pháp chính dùng phát hiện**
  - Dựa trên chữ ký (Signature-Based): Cơ chế phát hiện dựa trên chữ ký sử dụng các mã định danh duy nhất để tìm kiếm các mối đe dọa đã biết.

Ví dụ: IDS có thể có thư viện băm phần mềm độc hại mà nó sử dụng để xác định phần mềm độc hại đã biết đang cố gắng xâm nhập vào hệ thống được bảo vệ.

Intrusion Detection System - IDS

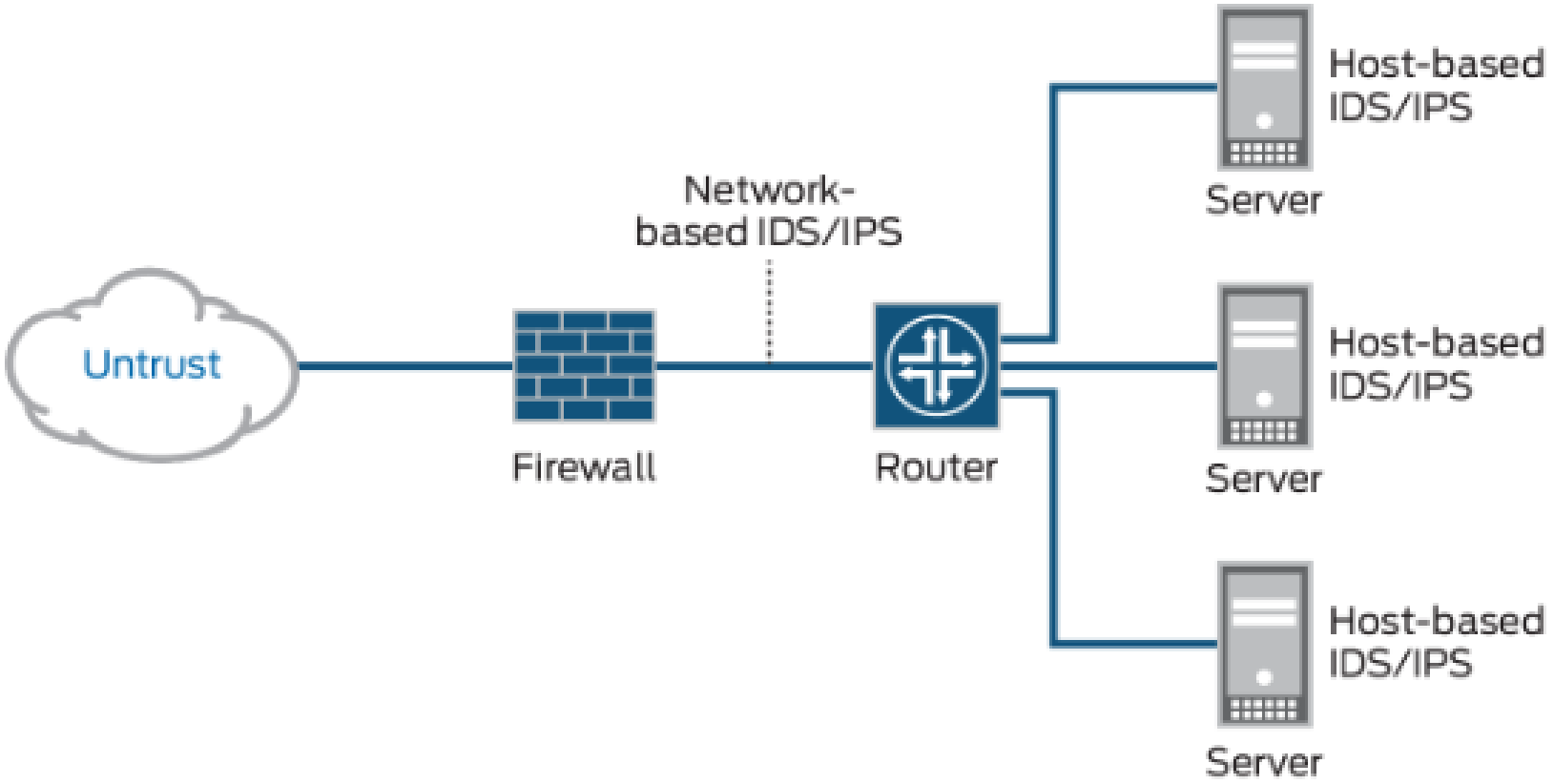
- **Phương pháp chính dùng phát hiện**
  - Dựa trên bất thường (Anomaly-Based): Phát hiện dựa trên bất thường phụ thuộc vào việc xây dựng mô hình về hành vi bình thường trong mạng hoặc thiết bị được bảo vệ. Sau đó, nó tìm kiếm bất kỳ sự sai lệch nào so với chuẩn mực này có thể chỉ ra một cuộc tấn công mạng hoặc sự cố khác.

Vị trí đặt IDS



https://telecom.qtsc.com.vn/Security/IPS_IDS

Vị trí đặt IDS



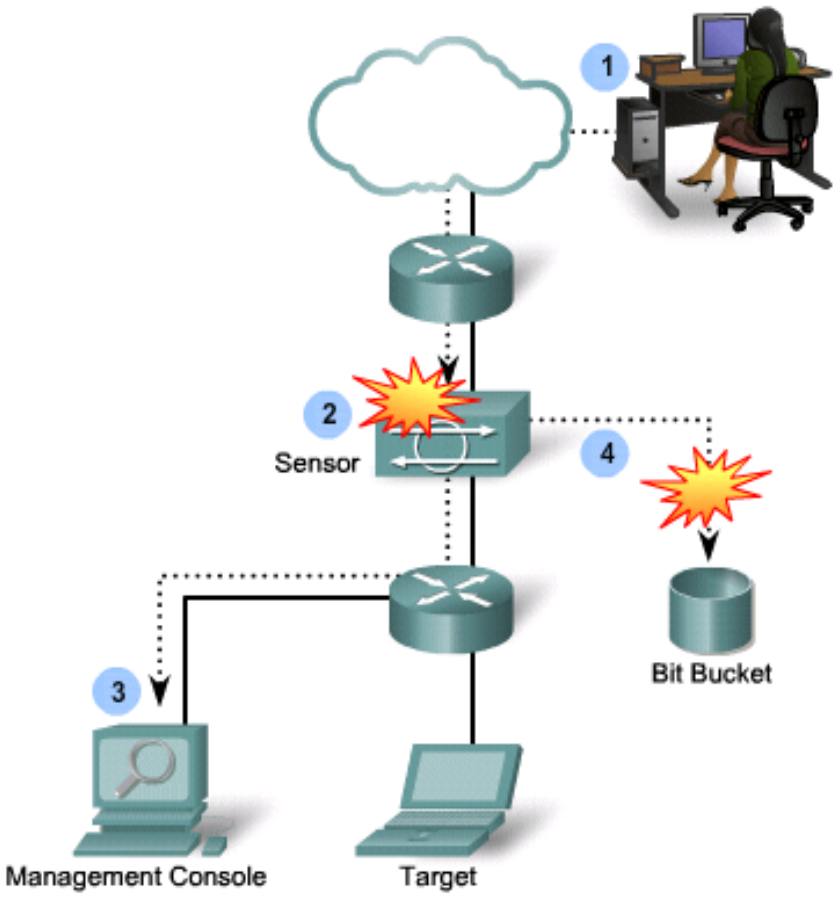
https://telecom.qtsc.com.vn/Security/IPS_IDS

Intrusion Detection System - IDS

- IDS sẽ chỉ đưa ra cảnh báo về một sự cố tiềm ẩn, từ đó, nhà phân tích Security Operations Center (SOC) sẽ điều tra và xác định xem có cần thực hiện thêm hành động nào không. Các loại IDS phổ biến là:
  - Network intrusion detection systems (NIDS): Giám sát lưu lượng truy cập thông qua các cảm biến khác nhau được đặt trên mạng.
  - Host intrusion detection systems (HIDS): Được đặt trực tiếp trên các thiết bị nhằm giám sát lưu lượng truy cập để quản trị viên mạng có nhiều quyền kiểm soát hơn.
  - Protocol-based intrusion detection systems (PIDS): Được đặt ở phía trước máy chủ và giám sát lưu lượng truy cập đến và đi từ các thiết bị.
  - Application protocol-based intrusion detection systems (APIDS): Giám sát lưu lượng truy cập trên một nhóm máy chủ.
  - Hybrid IDS: Là sự kết hợp của các loại hệ thống phát hiện xâm nhập nêu trên.

Intrusion Prevention Systems - IPS

Intrusion Prevention System - IPS



- **Một IPS** hoạt động chủ động bởi vì luồng lưu thông mạng phải đi qua nó.
  - Hoạt động ở chế độ "inline-mode", theo dõi lưu thông và nội dung từ tầng 2 đến tầng 7.
  - IPS có thể dừng các gói liên quan đến tấn công hệ thống đích (IDS thì không làm được điều này!)

Ngăn ngừa xâm nhập

- Là hoạt động có khả năng dừng các cuộc tấn công mạng và cung cấp các cơ chế phòng thủ:
  - **Detection** – Nhận diện các cuộc tấn công mạng và tài nguyên các máy trên mạng.
  - **Prevention** – Dừng các cuộc tấn công đang diễn ra.
  - **Reaction** – 'miễn dịch' cho hệ thống từ các cuộc tấn công mạng trong tương lai từ các nguồn đã phát hiện.
- Công nghệ có thể được cài đặt trên mạng, trên máy chủ hoặc cả hai để bảo vệ tối đa.

Các loại IPS

- **Network-based intrusion prevention systems** (NIPS) : Giám sát và bảo vệ toàn bộ mạng.
- **Host-based intrusion prevention systems** (HIPS): Được triển khai trên các thiết bị hoặc máy chủ quan trọng.
- **Wireless intrusion prevention systems** (WIPS): hệ thống ngăn chặn xâm nhập không dây.
- **Network behavioral analysis (NBA)**: phân tích hành vi mạng hay Distributed denial-of-service prevention (DDoS) – ngăn chặn tấn công từ chối dịch vụ phân tán.

Network-Based IPS (NIPS)

- Thực hiện phân tích hoạt động lưu thông trên toàn mạng để tìm các hoạt động không hợp pháp.
  - Được cấu hình dựa theo bộ quy tắc (**signatures**) để giám sát, có thể phát hiện ra các mẫu lưu thông bất thường.
- **Thiết bị:**
  - Thiết bị chuyên dụng IPS
  - ISR (Integrated Service Routers)
  - **Cisco ASA firewall appliances**
  - Cisco Catalyst 6500 network modules

Các đặc trưng Network-Based IPS (NIPS)

- Các 'bộ cảm biến' được kết nối với các đoạn mạng.
  - Một cảm biếm có thể giám sát được nhiều máy.
- Các 'bộ cảm biến' chuyên dụng có thể được điều chỉnh để phân tích phát hiện xâm nhập.
- Đảm bảo nhiệm vụ bảo vệ ngay cả khi mạng phát triển
  - Các máy tính và thiết bị mạng được lắp đặt thêm vào hệ thống nhưng không cần thêm các cảm biến.
  - Cảm biến mới có thể được dễ dàng thêm vào các nhánh mạng mới phát sinh.

Network-Based IPS (NIPS)

- **Network-based intrusion prevention system (NIPS):** Là loại IPS được triển khai trên một thiết bị riêng biệt.
- NIPS thường được đặt **trước hoặc sau** firewall để giám sát và bảo vệ toàn bộ mạng.
- NIPS có khả năng phân tích các gói tin truyền qua mạng và áp dụng các tập luật để ngăn chặn các gói tin có chứa mã độc, tấn công từ chối dịch vụ (DoS) hay tấn công khai thác lỗ hổng.

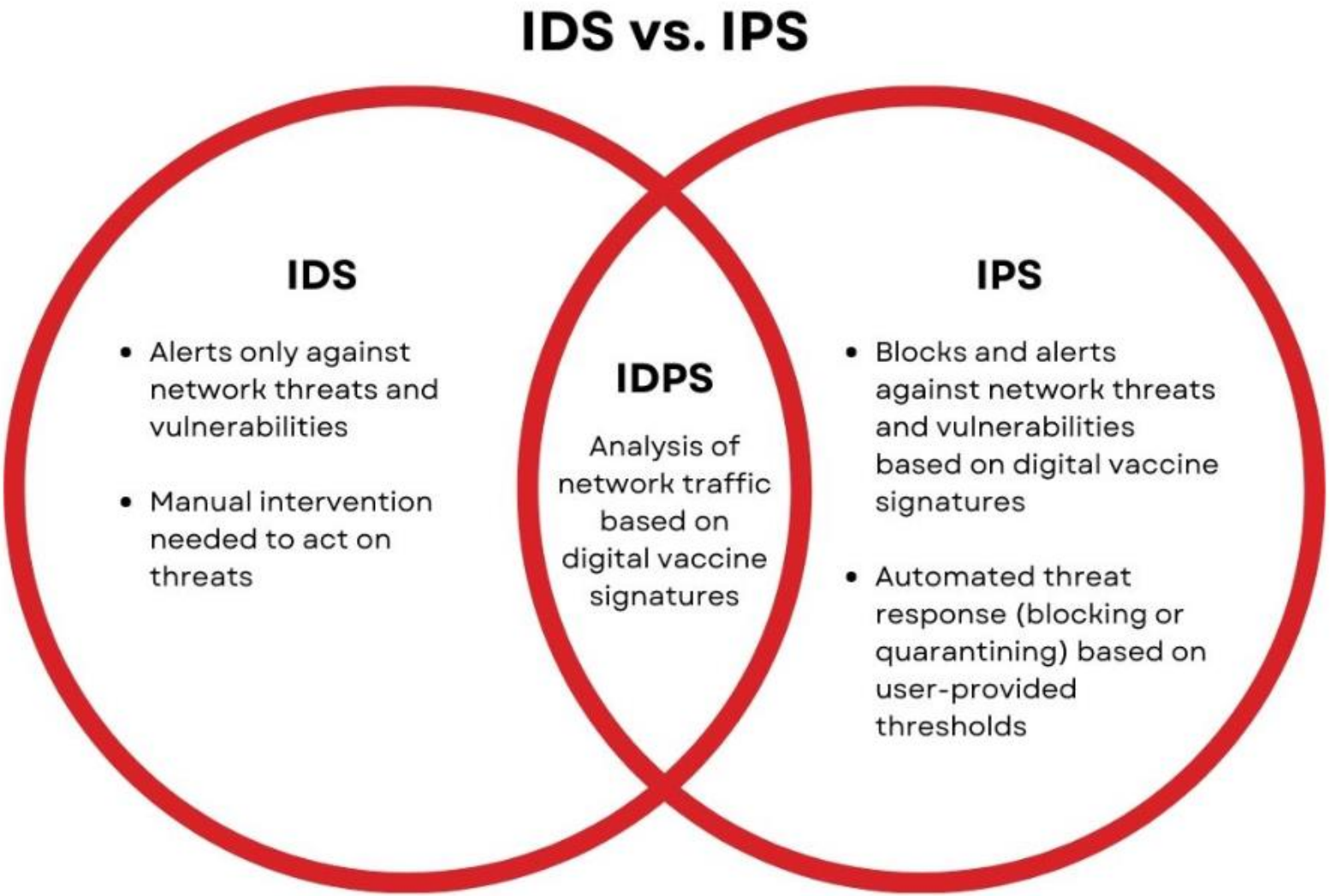
Host-based Intrusion Prevention System (HIPS)

- **HIPS:** Là loại IPS được triển khai trên một máy tính cá nhân hay máy chủ.
- **HIPS** thường được tích hợp với các phần mềm antivirus hay firewall cá nhân để giám sát và bảo vệ máy tính đó.
- **HIPS** có khả năng kiểm tra các hoạt động của các ứng dụng, tiến trình hay tập tin trên máy tính và áp dụng các tập luật để ngăn chặn các hoạt động có thể gây hại cho hệ thống, như cài đặt phần mềm độc hại, thay đổi cấu hình hay truy cập trái phép.

Comparing IDS and IPS Solutions

	IDS (Promiscuous Mode)	IPS (Inline Mode)
Advantages	• Không ảnh hưởng đến hiệu suất mạng (latency, jitter). • Không ảnh hưởng đến hoạt động của mạng ngay cả khi 'cảm biến' bị hư hỏng hay quá tải.	• Dừng tức thị các gói liên quan đến tấn công đang diễn ra.
Disadvantages	• Không thể dừng các cuộc tấn công đang diễn ra. • Trong quá trình hoạt động phải 'tinh chỉnh'. • Còn nhiều điểm yếu.	• Có ảnh hưởng đến hiệu suất mạng (latency, jitter). • Cảm biến bị hư hỏng hay quá tải sẽ ảnh hưởng nghiêm trọng đến hoạt động của hệ thống mạng.

IDPS = IDS + IPS



Lựa chọn IDS hay IPS?

- Các kỹ thuật này không loại trừ nhau
- IDS và IPS có thể được cài đặt để bổ sung cho nhau.

  Ví dụ: một IDS có thể được thực hiện để xác nhận hoạt động IPS, vì IDS có thể được cấu hình cho kiểm tra gói tin đã diễn ra (offline) sâu hơn, điều này cho phép các IPS tập trung vào các mẫu đang lưu thông (inline)
- Quyết định cài đặt giải pháp công nghệ nào phải được dựa trên các mục tiêu an ninh nêu trong chính sách an ninh mạng.

Chức năng IDS/IPS và Firewall

- **IDS** giám sát và phát hiện các hoạt động xâm nhập hoặc không chính thức trên mạng hoặc hệ thống máy tính và tạo ra cảnh báo khi phát hiện các sự kiện đáng ngờ.
- **IPS** không chỉ phát hiện mà còn ngăn chặn các hoạt động xâm nhập hoặc không chính thức bằng cách áp dụng các biện pháp phòng ngừa hoặc ngăn chặn tự động.

Chức năng IDS/IPS và Firewall

- **Firewall** là một hệ thống bảo vệ an ninh mạng, kiểm soát lưu lượng mạng và quyết định xem liệu gói tin dữ liệu có được chuyển tiếp hay không dựa trên các quy tắc định trước.
- Có thể kết hợp chức năng Firewall với IPS hoặc IDS để tăng cường khả năng bảo mật hệ thống.

https://fptshop.com.vn/tin-tuc/danh-gia/ids-la-gi-bat-mi-su-khac-biet-giua-ids-va-ips-tuong-lua-qua-nhung-kien-thuc-huu-ich-168414

Tham khảo

- Cisco IPS
  - www.cisco.com/go/ips
- Shields Up! Time to Start Blocking with your Cisco IPS Sensors
  - http://www.networkworld.com/community/node/45922
- Cisco IPS Sensor Tuning Timesavers
  - http://www.networkworld.com/community/node/55244?source=NWWNLE_nlt_cisco_2010-01-18
- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.geeksforgeeks.org/intrusion-prevention-system-ips/
- https://www.trendmicro.com/en_us/ciso/22/l/intrusion-detection-prevention-systems.html
- https://fptshop.com.vn/tin-tuc/danh-gia/ids-la-gi-bat-mi-su-khac-biet-giua-ids-va-ips-tuong-lua-qua-nhung-kien-thuc-huu-ich-168414