CHƯƠNG 5
PHÁT HIỆN XÂM NHẬP TRÁI PHÉP

Giảng viên:

Trần Thị Lượng

Nội dung - Phần I

1. Tại sao phải bảo mật CSDL?
2. Các tấn công vào CSDL
   2.1 Tấn công tính bí mật
   2.2 Tấn công tính toàn vẹn
3. Mô hình đe dọa
4. Đảm bảo an toàn CSDL bằng mật mã

Nội dung - Phần II

1. Một số kiểu tấn công mạng cơ bản
2. Tổng quan về hệ thống IDS
3. Kiến trúc chung của hệ thống IPS, IDS
4. Mô hình, cấu trúc và hoạt động của hệ thống IPS, IDS

Phần I

1. Tại sao phải bảo mật CSDL?
2. Các tấn công vào CSDL
   2.1 Tấn công tính bí mật
   2.2 Tấn công tính toàn vẹn
3. Mô hình đe dọa
4. Đảm bảo an toàn CSDL bằng mật mã

1. Tại sao phải bảo mật CSDL?

- Một CSDL cung cấp những thông tin quan trọng của khách hàng, kế hoạch phát triển của một doanh nghiệp, các dự đoán kinh tế, và nhiều mục đích quan trọng khác…
- Sẽ có lợi cho một tin tặc khi tấn công vào CSDL hơn là nghe nén giao tiếp trên mạng.
- Dữ liệu thường được mã hóa trên đường truyền nhưng lại lưu dưới dạng rõ trong CSDL.
- Sự cố về an ninh xảy ra với CSDL có thể ảnh hưởng nghiêm trọng đến danh tiếng của công ty và quan hệ với khách hàng.

2. Các tấn công vào CSDL

- ***Tấn công bên trong:*** tin tặc là người bên trong tổ chức (bên trong firewall), biết về kiến trúc của mạng.
- ***Tấn công bên ngoài***: tin tặc phải vượt qua firewall, IDS và không biết về kiến trúc của mạng

=> Các tin tặc bên trong (có thể gồm cả admin của CSDL) là mối đe dọa còn lớn hơn các tấn công bên ngoài.

2.1 Tấn công tính bí mật

- ***Định nghĩa:*** Là loại tấn công trong đó, những người dùng bất hợp pháp có khả năng truy nhập vào thông tin nhạy cảm của CSDL.
  - Kiểm soát mức thấp nhất là đọc CSDL.
- ***Ví dụ:*** tin tặc có thể kiểm soát toàn bộ máy chủ CSDL, do đó anh ta có thể
  - Download toàn bộ file CSDL.
  - Nạp file vào Database engine để truy nhập dữ liệu như người dùng bình thường.

2.1 Tấn công tính bí mật

- ***Kiểm soát truy nhập:*** thường được sử dụng để bảo vệ CSDL, nhưng chưa đủ!
  - Thường được cấu hình chưa đúng
  - Tạo khe hở (backdoor) cho những người dùng muốn lạm dùng quyền.
- ***Việc backup CSDL không an toàn:*** là một khả năng cho kẻ tấn công có thể truy nhập vào dữ liệu nhạy cảm.

2.1 Tấn công tính bí mật

- ***Lỗi SQL Injection:*** do người lập trình yếu, tạo khe hở để kẻ tấn công truy nhập trái phép CSDL (thường trong các ứng dụng Web).
- ***Truy nhập vào file CSDL vật lý***

2.1 Tấn công tính bí mật

- ***Giải pháp:***
  - Mã hóa file CSDL, mã hóa CSDL (các bảng, khung nhìn…những thông tin bí mật).
  - Áp dụng các cơ chế bảo vệ mức cao cho bản thân CSDL.

2.2 Tấn công tính toàn vẹn

- ***Định nghĩa:*** Là loại tấn công gây ra những sửa đổi trái phép đối với thông tin trong CSDL.
  - Yêu cầu: kẻ tấn công phải có khả năng Write CSDL.
  - Do đó, ta không lo ngại đối với các tin tặc có thể đọc CSDL (trong loại tấn công này).

2.2 Tấn công tính toàn vẹn

- ***Một số tấn công tính toàn vẹn phổ biến:***
  - Tấn công từ các admin ác ý
  - Sự gây hại của các ứng dụng bị lỗi
  - Sử dụng tài khoản đánh cắp có truy nhập write CSDL.
  - Khả năng leo thang đặc quyền của một số tài khỏan (escalating privileges)

2.2 Tấn công tính toàn vẹn

- ***Giải pháp:***
  - ***Tách bạch nhiệm vụ (Separaton of duties):*** Nguyên tắc này được đưa ra nhằm hạn chế tối đa một cá nhân bất kỳ có thể phá hoại dữ liệu, để đảm bảo toàn vẹn dữ liệu. Tách bạch nhiệm vụ được gắn liền với các kiểm soát trên các chuỗi giao tác. Để chuỗi này hoàn thành phải có nhiều hơn một người tham gia (Ví dụ giao dịch ngân hàng).
  - Chỉ những ***người dùng hợp pháp*** mới được phép thực hiện những ***ứng dụng (đã được phê duyệt)*** để thay đổi thông tin trong CSDL.

3. Mô hình đe dọa

- Mô hình này được xây dựng dựa trên các ***điểm yếu*** và những ***mối đe dọa*** khai thác các điểm yếu này.
- Một mô hình được tạo ra dễ dàng trong quá trình phát triển của hệ CSDL.
- Mô hình này ảnh hưởng đến kiến trúc và thiết kế của hệ thống đó.
- Các nguyên lý mật mã và các giao thức an toàn được lựa chọn để làm giảm bớt các mối đe dọa trên.

3. Mô hình đe dọa

- Dựa vào các tấn công đã thảo luận, mô hình đe dọa bao gồm các mối đe dọa sau:

  *1. Các nhà quản trị CSDL (*database administrators*)*

  *2. Nhân viên phát triển (*development staff*)*

  *3. Những kẻ xâm nhập qua mạng (*network intruders)

  *4. Những người dùng hợp pháp (*legitimate users)

  *5. Các cracker ứng dụng (*application crackers)

  *6. Những kẻ ăn trộm truyền thống (*traditional thieves)

3.1 Các nhà quản trị CSDL

- ***Đặc điểm:***
  - Là những người dùng có đặc quyền truy nhập vào mọi thứ trong miền quản trị của họ.
  - Có khả năng truy nhập mọi thông tin trong CSDL.
  - Có thể che giấu những dấu vết tấn công
- ***Ngăn chặn***:
  - Tách bạch nhiệm vụ (phân vùng công việc), mã hóa thông tin, ghi nhật ký

3.2 Nhân viên phát triển

- ***Đặc điểm:***
  - Chịu trách nhiệm thiết kế, xây dựng và kiểm thử các ứng dụng CSDL.
  - Là những người am hiểu rất tốt về hệ thống CSDL.
  - Có thể truy nhập vào các tài khoản để sửa chữa sự cố.
- ***Ngăn chặn:***
  - Mã hóa thông tin, ghi nhật ký.

3.3 Kẻ xâm nhập qua mạng

- ***Đặc điểm:***
  - Là những cá nhân truy nhập bất hợp pháp qua mạng.
  - Nghe trộm giao tiếp trên mạng để thu được thông tin mật hoặc các giấy ủy nhiệm xác thực nào đó.
  - Những người này có thể cố gắng phá các ứng dụng CSDL.
- ***Ngăn chặn:***
  - Mã hóa đường truyền, dùng các IDS và các ứng dụng đã được cứng hóa.

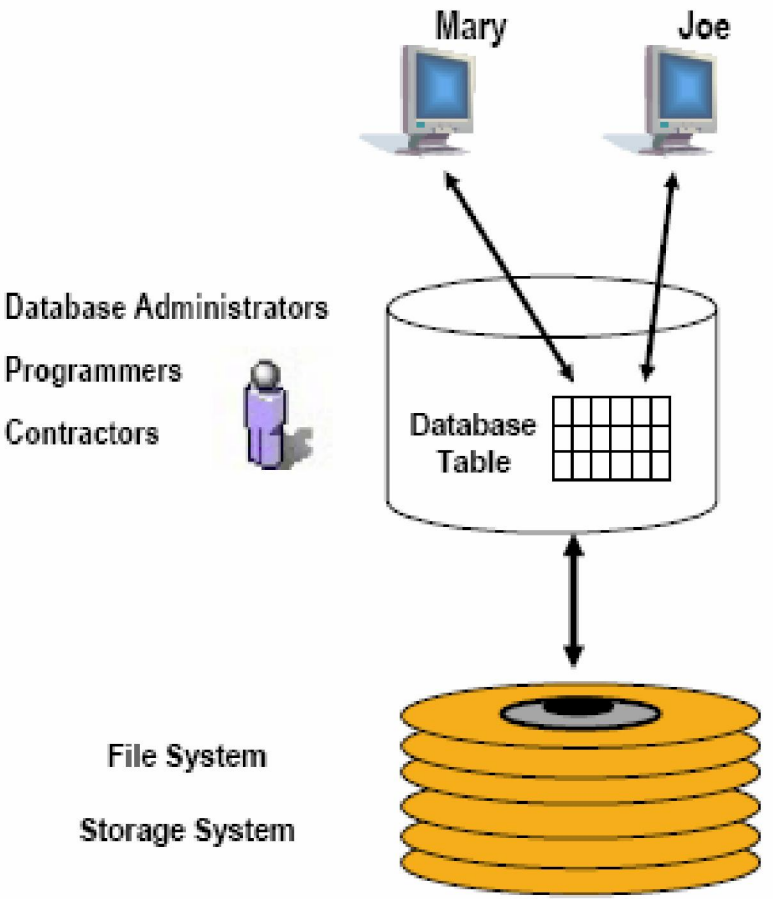
3.4 Các cracker ứng dụng

- ***Đặc điểm:***
  - Các cracker cố gắng phá vỡ an toàn ứng dụng để giành được các truy nhập bất hợp pháp vào CSDL.
  - Trường hợp xấu nhất là cracker có thể thu được các đặc quyền quản trị.
- ***Ngăn chặn:***
  - Dùng IDS, ngăn chặn SQL injection, cứng hóa các ứng dụng.

3.5 Người dùng hợp pháp và kẻ ăn trộm truyền thống

- ***Người dùng hợp pháp:***
  - Cố gắng lạm dụng quyền của mình để thu được những truy nhập thêm (bất hợp pháp)
  - Hành động rất giống các cracker ứng dụng
- ***Kẻ ăn trộm truyền thống:***
  - Có thể đánh cắp CSDL hoặc bản sao CSDL.
- ***Ngăn chặn:***
  - Đảm bảo an toàn cho máy chủ CSDL và các phương tiện sao lưu.

Các mối đe dọa đến CSDL và hệ thống file



Database Threats

- ✓Hackers
- ✓Employees,
- ✓Contractors
- ✓Customers
- ✓Suppliers
- ✓Partners
- ✓Outsourcers
- ✓Trojan Horses
- ✓Application errors

File System Threats

- ✓Physical Theft – file / backup
- ✓Root/Admin

4. Đảm bảo an toàn CSDL bằng mật mã

- Dùng ***mật mã đối xứng*** để đảm bảo an toàn cho dữ liệu nhạy cảm.
- Chuyển từ bài toán bảo vệ dữ liệu sang bài toán bảo vệ ***khóa bí mật***.
  - Dễ dàng bảo vệ một khóa hơn là nhiều khóa.
- Bảo vệ khóa từ truy nhập ***trực tiếp*** và ***gián tiếp***.

4.1 Truy nhập khóa trực tiếp

- ***Đặc điểm:***
  - Một tin tặc với truy nhập trực tiếp vào khóa, có thể sao chép và sử dụng khóa để giải mã thông tin.
- ***Ngăn chặn:***
  - Để bảo vệ khóa khỏi mọi đe dọa, cần lưu khóa vào một Modul phần cứng an toàn (HSM)
  - Nếu không sử dụng HSM, thì cần thiết lưu các khóa ở những nơi riêng biệt trong CSDL.

4.2 Truy nhập khóa gián tiếp

- ***Đặc điểm:***
  - Thay vì tấn công khóa trực tiếp, tin tặc tấn công một ứng dụng (có thể truy nhập khóa) để giải mã thông tin mật.
  - Là một mối đe dọa nghiêm trọng vì kẻ tấn công vẫn lấy được thông tin nhạy cảm dù khóa đã được thay đổi.
  - Khó khăn hơn nhiều trong việc ngăn chặn tấn công này so với tấn công khóa trực tiếp.

4.2 Truy nhập khóa gián tiếp

- ***Ngăn chặn:***
  - Kiểm soát truy nhập mạnh (nhận dạng, xác thực) đối với mỗi yêu cầu giải mã dữ liệu.
  - Giải mã ít nhất các cột cần thiết trong CSDL.
  - Đăng nhập mở rộng đối với các yêu cầu giải mã.

4.3 Rủi ro khi mã hóa

- Rủi ro lớn nhất có lẽ là mất các khóa
  - Dẫn đến mất toàn bộ dữ liệu
- Quá trình sinh khóa không đủ ngẫu nhiên
  - Dẫn đến có thể ‘dễ dàng đoán’ các khóa
- Thực thi mã hóa gặp sự cố
  - Dẫn đến mã hóa ‘tồi’

Phần II

1. Một số kiểu tấn công mạng cơ bản
2. Tổng quan về hệ thống IDS
3. Kiến trúc chung của hệ thống IPS, IDS
4. Mô hình, cấu trúc và hoạt động của hệ thống IPS, IDS

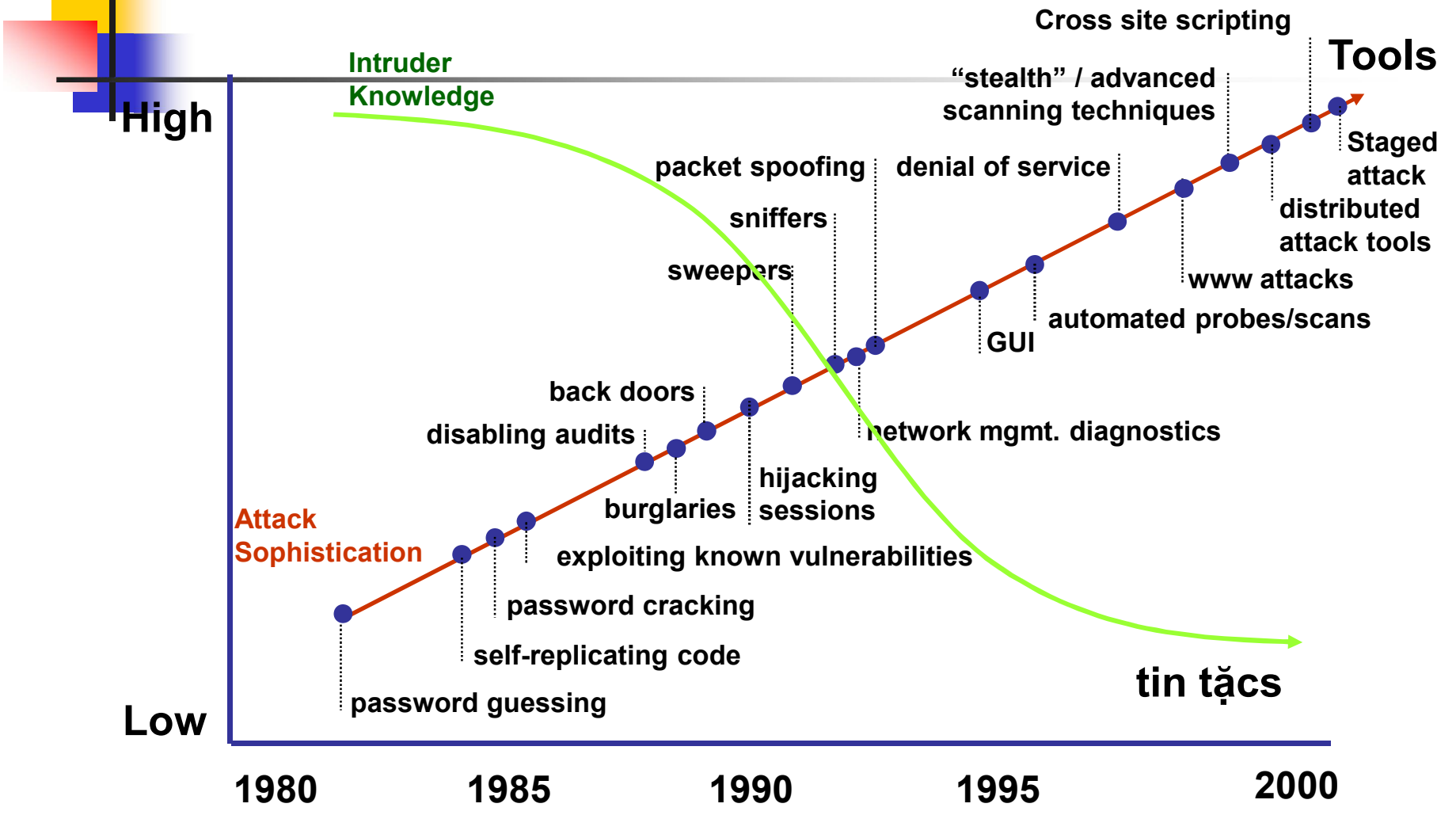
Viết tắt

- ***IDS:*** Intrusion Detection System (Hệ thống phát hiện xâm nhập)
- ***IPS:*** Intrusion Prevention System (Hệ thống ngăn chặn xâm nhập)

1. Một số kiểu tấn công cơ bản

- Các hành vi dò quét.
- Các tấn công từ chối dịch vụ (DoS).
- Các hành vi khai thác lỗ hổng bảo mật.
- Các tấn công con ngựa thành Tơroa
- Các tấn công mức ứng dụng

Attack Sophistication vs. Intruder Technical Knowledge



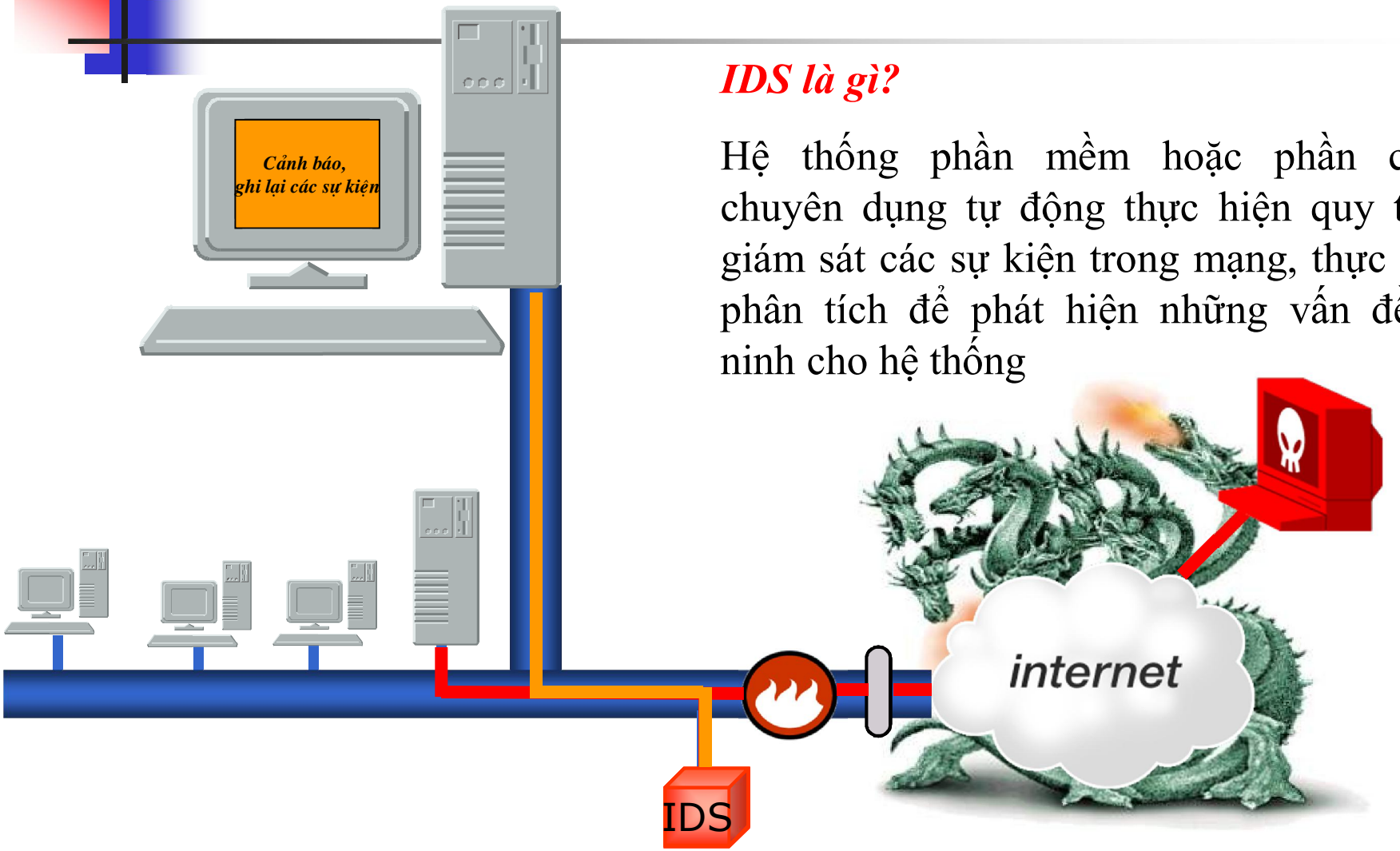
Copyright: CERT, 2000

2. Tổng quan về hệ thống IDS

- ***Các hệ thống an ninh mạng truyền thống:***
  - Chỉ dựa trên các firewall để kiểm sóat luồng thông tin vào ra
  - Firewall chỉ kiểm soát được các luồng thông tin đi qua nó
  - Dựa trên các luật cố định
  - Không chống được: virus, giả danh, khai thác thông tin trái phép trên mạng (ví dụ: sniffer),…

  => Không chống được các kiểu tấn công mới
- ***Kỹ thuật an ninh mới:***
  - Kết hợp Firewall+IDS => IPS (hệ thống ngăn chặn xâm nhập): có khả năng phát hiện các cuộc tấn công và tự động ngăn chặn các cuộc tấn công đó.

2. Tổng quan về hệ thống phát hiện xâm nhập - IDS



IDS là gì?

Hệ thống phần mềm hoặc phần cứng chuyên dụng tự động thực hiện quy trình giám sát các sự kiện trong mạng, thực hiện phân tích để phát hiện những vấn đề an ninh cho hệ thống

2. Tổng quan về hệ thống IDS

- ***Chức năng của IDS***
  - Phát hiện xâm nhập trái phép vào hệ thống mạng, đây là chức năng chính của IDS.
  - Tăng khả năng giám sát các hoạt động trên mạng
  - Cảnh báo, hỗ trợ ngăn chặn tấn công

2. Tổng quan về hệ thống IDS

- ***Ưu điểm của IDS:***
  - Có khả năng phát hiện các cuộc tấn công, xâm nhập từ bên trong cũng như bên ngoài hệ thống.
  - Những thông tin hệ thống IDS cung cấp sẽ giúp chúng ta xác định phương thức, và kiểu loại tấn công, xâm nhập => đưa ra phương án phòng chống.

2. Tổng quan về hệ thống IDS

- ***Nhược điểm:***
  - IDS là một hệ thống giám sát thụ động, cơ chế ngăn chặn các cuộc tấn công, xâm nhập trái phép rất hạn chế ***(Không chống được tấn công).***
  - Phần lớn, hệ thống IDS sẽ đưa ra các cảnh báo khi các cuộc tấn công, xâm nhập đã ảnh hưởng tới hệ thống rồi!

=> *Cần kết hợp IDS với tường lửa và IPS.*

3. Kiến trúc chung của hệ thống IDS

3.1 Hệ thống IDS trên máy trạm

(***HIDS*** – Host based-IDS)

3.2 Hệ thống IDS trên mạng

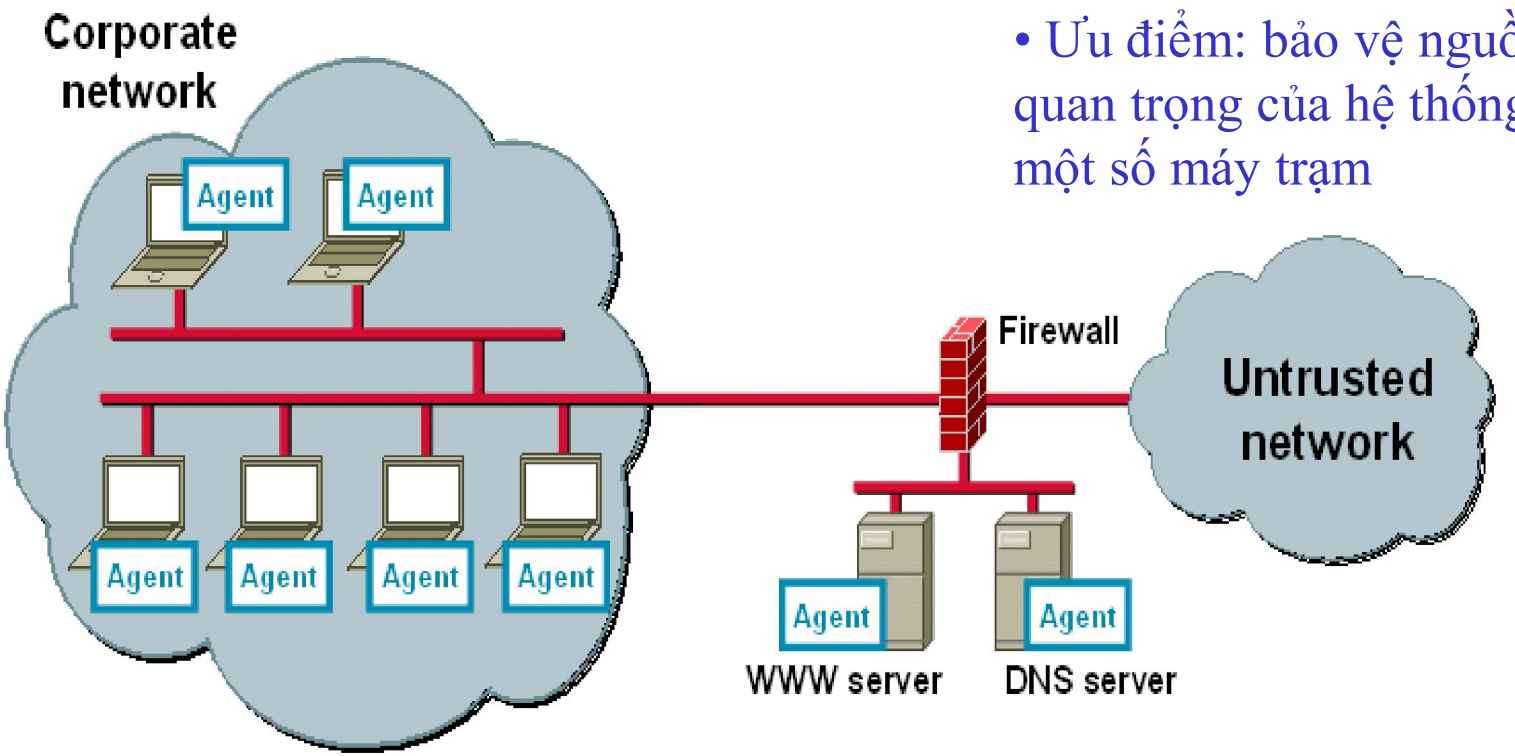
(***NIDS*** – Network based – IDS)

3.3 So sánh giữa HIDS và NIDS

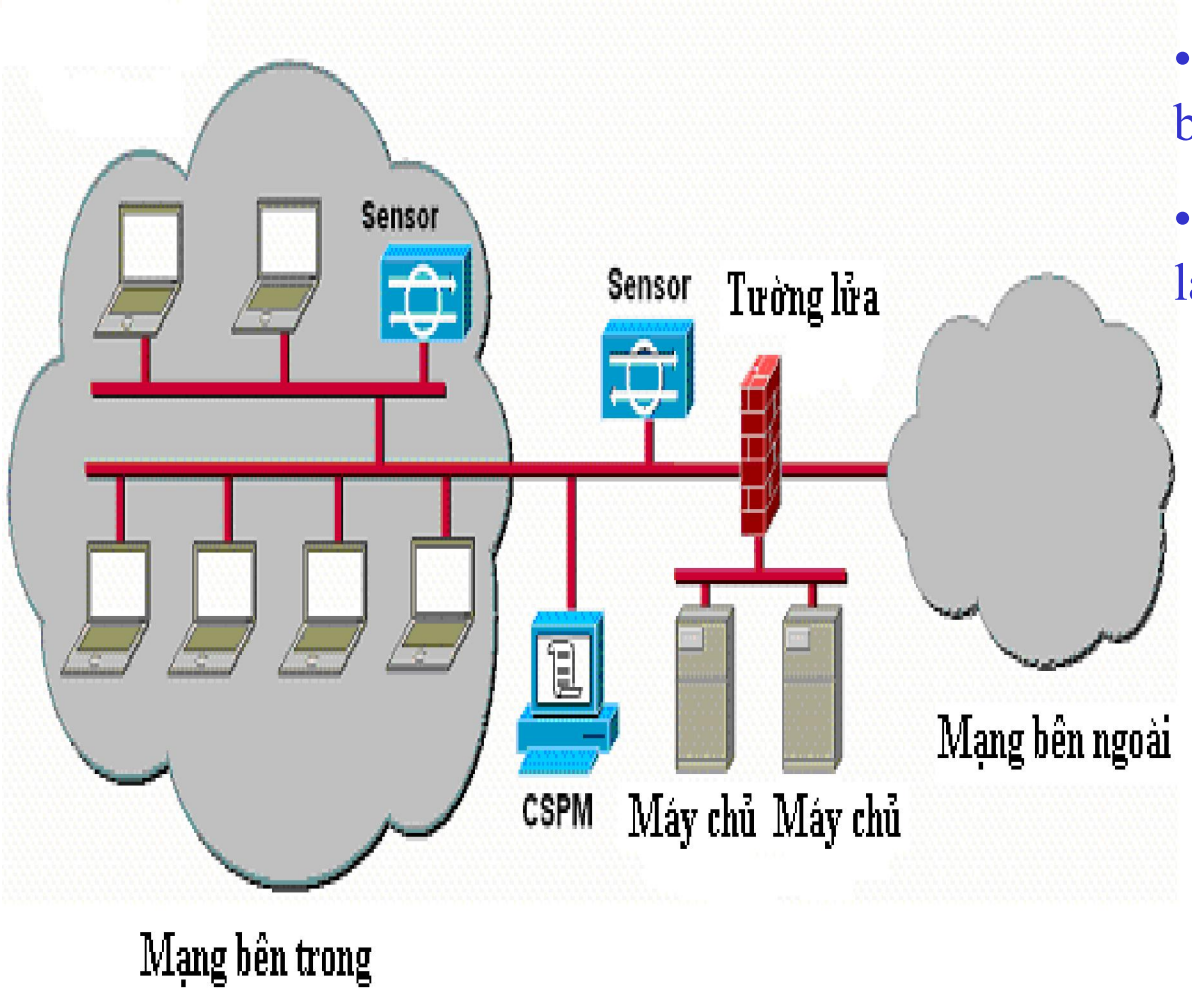
3.4 Mô hình, cấu trúc, hoạt động của IPS, IDS

3.1 Hệ thống IDS trên máy trạm (HIDS)

- Triển khai trên các máy riêng lẻ
- Phụ thuộc vào hệ điều hành.
- Ưu điểm: bảo vệ nguồn tài nguyên quan trọng của hệ thống chỉ lưu trên một số máy trạm



3.2 Hệ thống IDS trên mạng (NIDS)



- Triển khai bảo vệ cho toàn bộ hệ thống mạng
- Ưu điểm: phạm vi rộng, độc lập với hệ điều hành

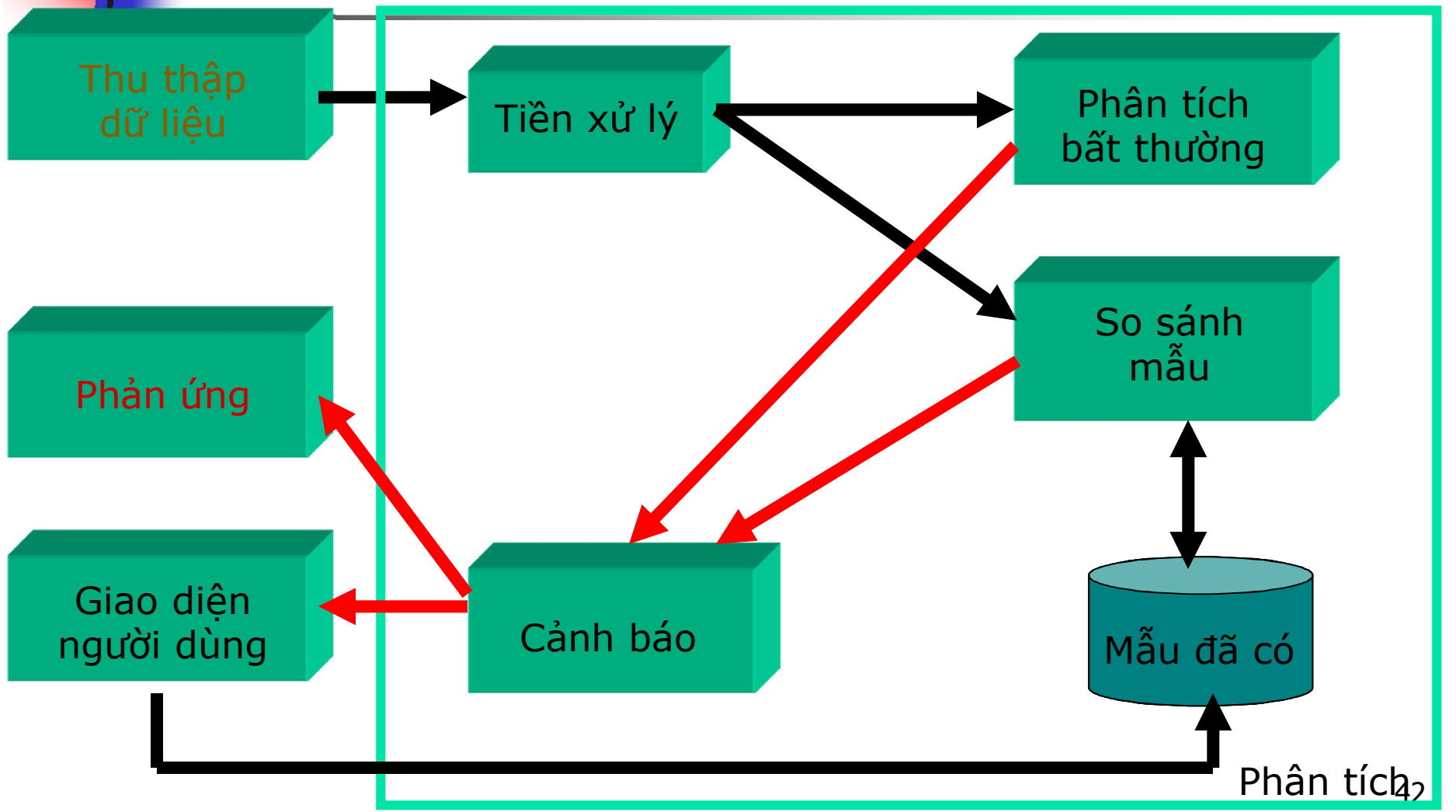
3.3 So sánh giữa HIDS và NIDS

- Bài tập?

3.4 Mô hình, cấu trúc, hoạt động của IPS, IDS

- Một hệ thống IPS được xem là thành công nếu chúng hội tụ được các yếu tố:
  - Thực hiện nhanh, chính xác.
  - Đưa ra các thông báo hợp lý.
  - Phân tích được toàn bộ thông lượng, cảm biến tối đa.
  - Ngăn chặn thành công và chính sách quản lý mềm dẻo.
- Hệ thống IPS gồm 3 modul chính:
  - Modul thu thập thông tin, dữ liệu
  - Modul phân tích, phát hiện tấn công
  - Modul phản ứng

Cấu trúc bên trong hệ thống IPS



Modul thu thập dữ liệu

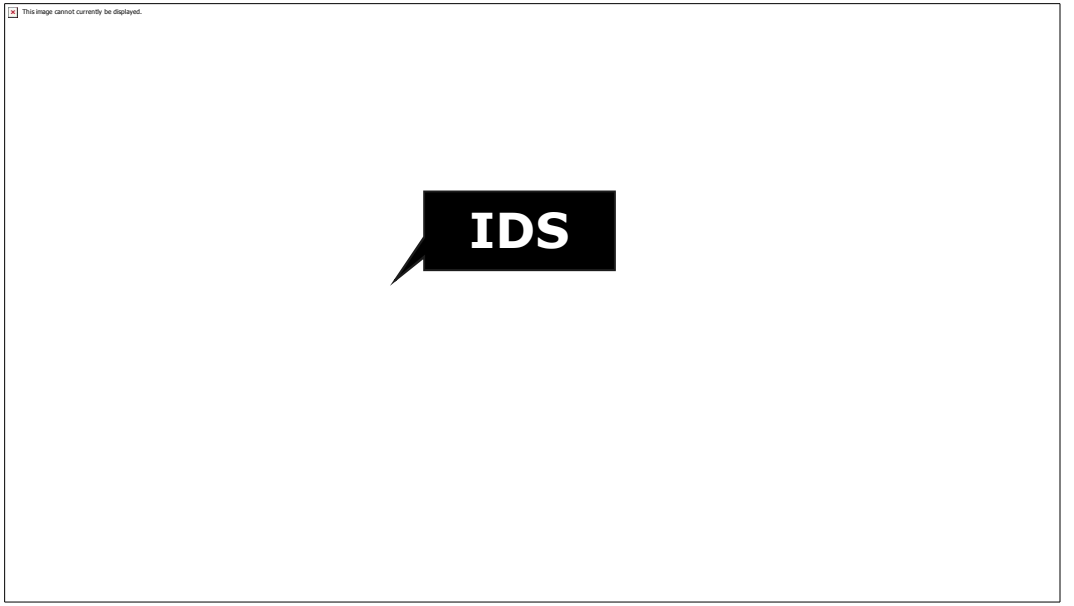
- Modul này có nhiệm vụ lấy tất các gói tin đi đến mạng để phân tích.
- Thông thường các gói tin có địa chỉ không phải của một card mạng thì sẽ bị huỷ bỏ nhưng card mạng của IPS được đặt ở chế độ thu nhận tất cả. Tất cả các gói tin qua chúng đều được sao chụp, xử lý, phân tích đến từng trường thông tin.
- Bộ phân tích đọc thông tin từng trường trong gói tin, xác định chúng thuộc kiểu gói tin nào, dịch vụ gì... Các thông tin này được chuyển đến ***modul phát hiện tấn công.***

Modul thu thập dữ liệu

- ***Mô hình thu thập dữ liệu ngoài luồng***
  - IDS không can thiệp trực tiếp vào luồng dữ liệu. Luồng dữ liệu vào ra hệ thống mạng sẽ được sao thành một bản và được chuyển tới modul thu thập dữ liệu.
  - Luồng dữ liệu vào hệ thống mạng sẽ cùng đi qua firewall và IPS.
  - IPS có thể kiểm soát luồng dữ liệu vào, phân tích và phát hiện các dấu hiệu của sự xâm nhập, tấn công. Với vị trí này, IPS có thể quản lý bức tường lửa, chỉ dẫn nó chặn lại các hành động đáng ngờ.
  - ***Ưu điểm:*** không ảnh hưởng đến lưu thông mạng.

Modul thu thập dữ liệu

- ***Mô hình thu thập dữ liệu ngoài luồng***

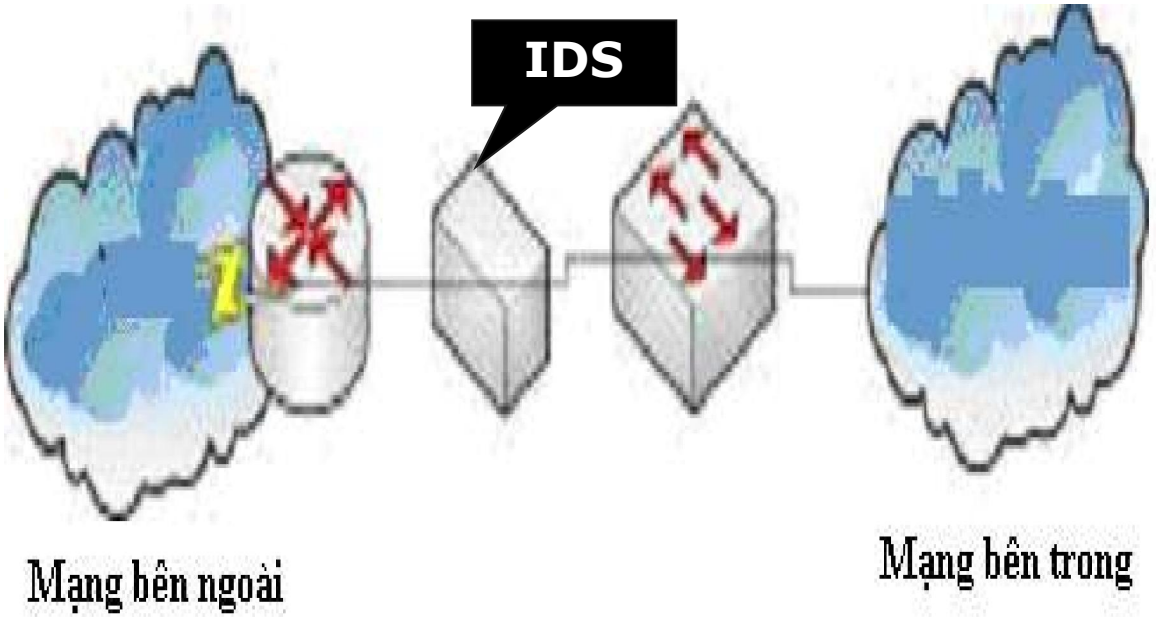


Modul thu thập dữ liệu

- ***Mô hình thu thập dữ liệu trong luồng***
  - Hệ thống IDS được đặt trực tiếp vào luồng dữ liệu vào/ra trong hệ thống mạng, luồng dữ liệu phải đi qua IDS trước khi đi vào mạng bên trong.
  - ***Ưu điểm:*** IDS nằm trên luồng dữ liệu, nó trực tiếp kiểm soát luồng dữ liệu, đáp ứng được thời gian thực (realtime).
  - ***Nhược điểm:*** ảnh hưởng đáng kể đến tốc độ lưu thông của mạng.

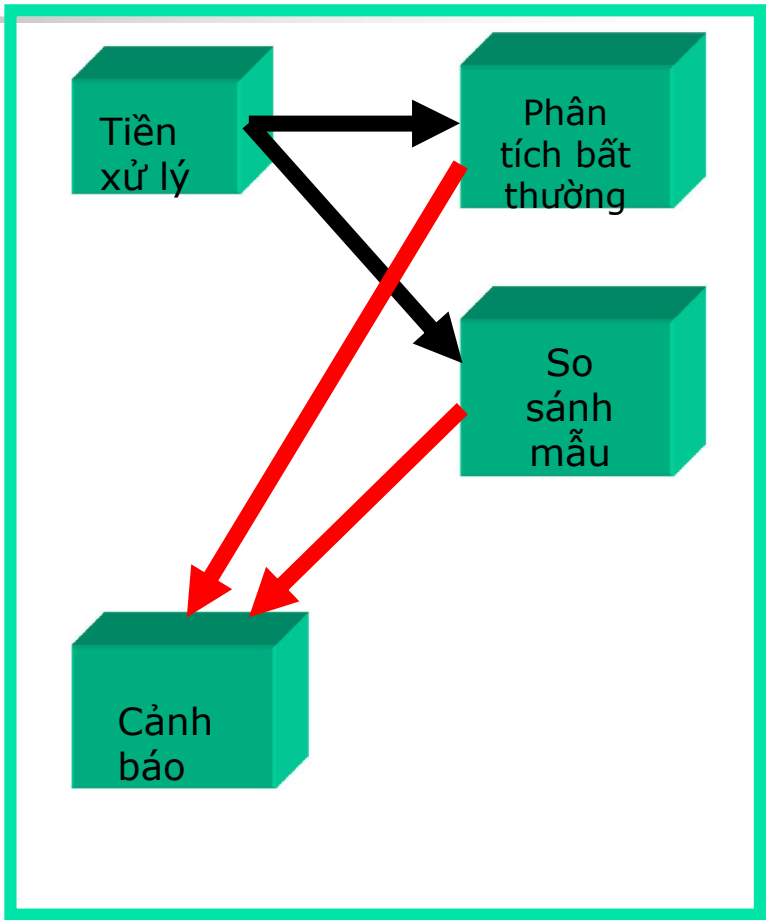
Modul thu thập dữ liệu

- *Mô hình thu thập dữ liệu trong luồng*



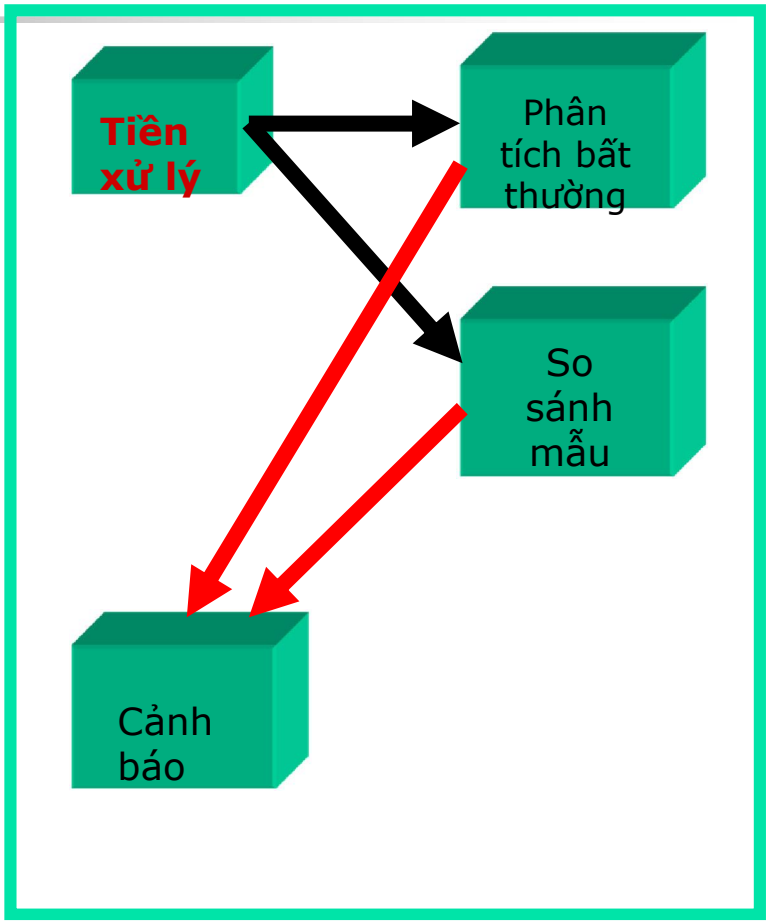
Modul phân tích, phát hiện tấn công

- Đây là modul quan trọng nhất nó có nhiệm vụ phát hiện các tấn công. Modul này đợc chia thành các giai đoạn:
  - Tiền xử lý
  - Phân tích
  - Cảnh báo.



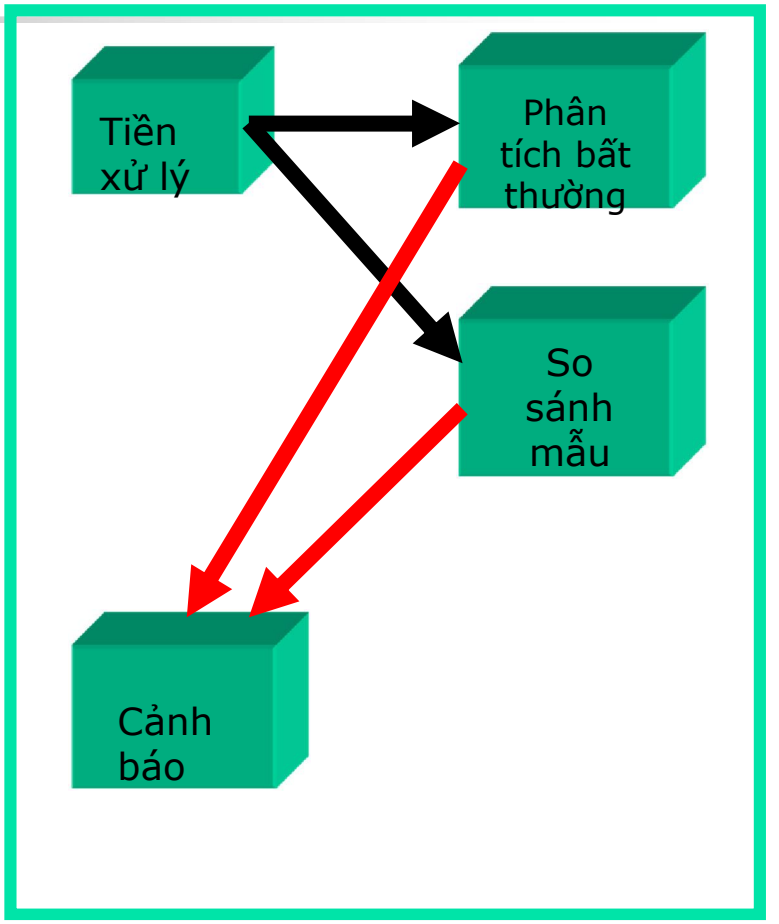
Modul phân tích, phát hiện tấn công

- ***Tiền xử lý:*** (tập hợp dữ liệu, tái định dạng gói tin):
  - Dữ liệu được sắp xếp theo từng phân loại, phân lớp.
  - Xác định định dạng của của dữ liệu đưa vào (chúng sẽ được chia nhỏ theo từng phân loại).
  - Ngoài ra, nó có thể tái định dạng gói tin (defragment), sắp xếp theo chuỗi.



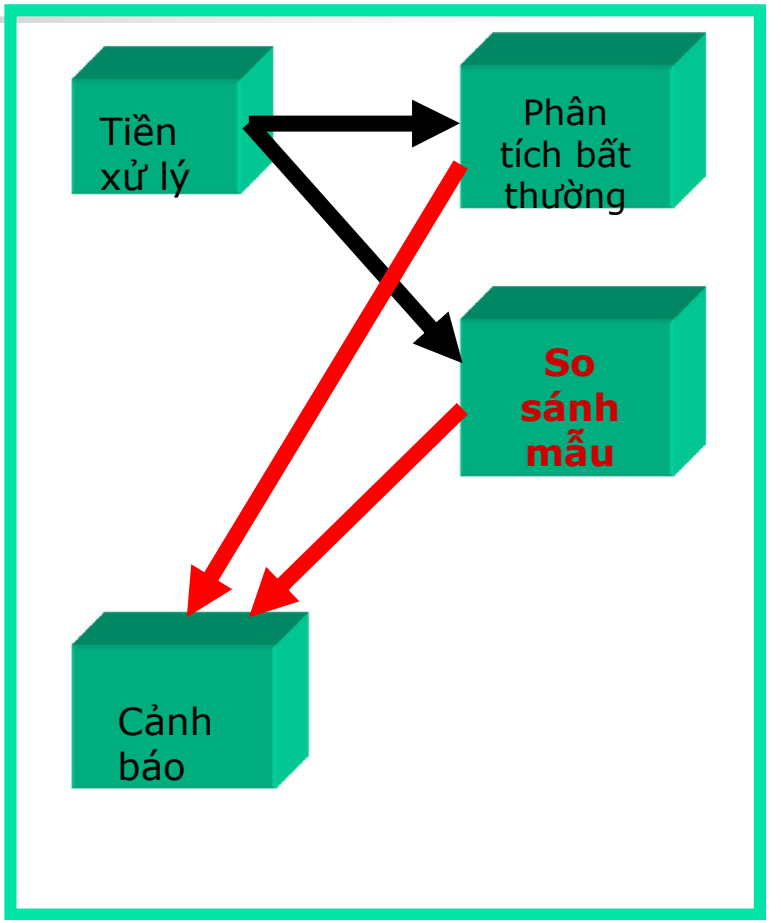
Modul phân tích phát hiện tấn công

- ***Phân tích:*** Dựa trên hai phương pháp phát hiện xâm nhập:
  - ***Phát hiện sự lạm dụng*** (*Misuse detection models*): Dựa trên mẫu, -u điểm chính xác
  - ***Phát hiện tình trạng bất thường*** (*Anomaly detection models*):



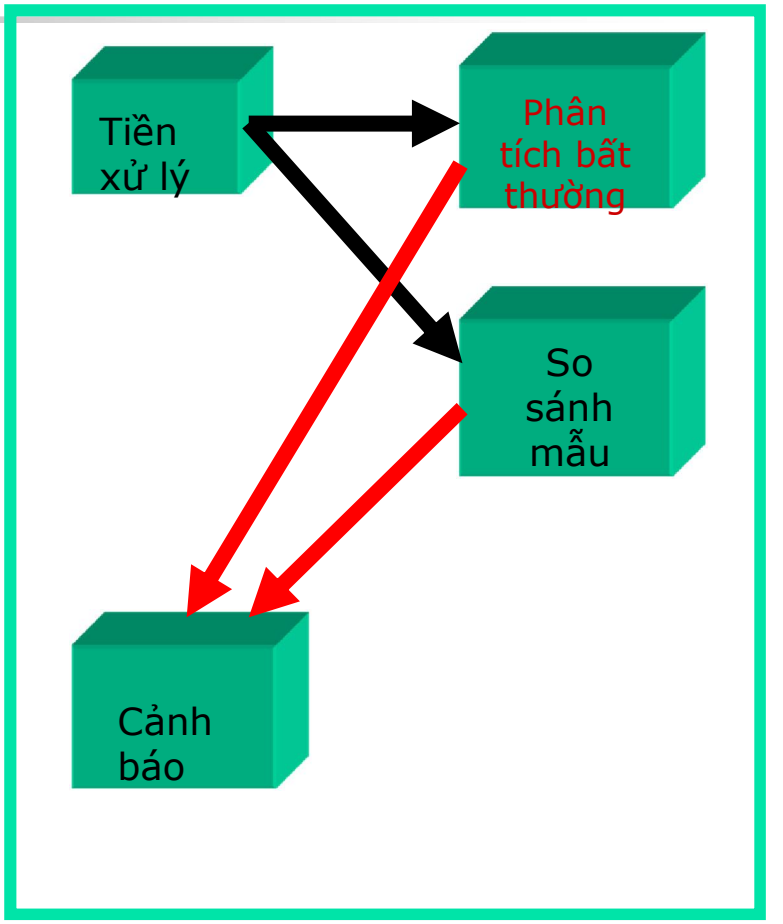
Modul phân tích phát hiện tấn công

- ***Phát hiện sự lạm dụng (Misuse detection models):***
  - Phân tích các hoạt động của hệ thống, tìm kiếm các sự kiện giống với các ***mẫu tấn công*** đã biết trước.
  - ***Ưu điểm:*** phát hiện các cuộc tấn công nhanh và chính xác, không đưa ra các cảnh báo sai làm giảm khả năng hoạt động của mạng và giúp các người quản trị xác định các lỗ hổng bảo mật trong hệ thống của mình.
  - ***Nhược điểm:*** là không phát hiện được các cuộc tấn công không có trong cơ sở dữ liệu, các kiểu tấn công mới, do vậy hệ thống luôn phải cập nhật các mẫu tấn công mới.



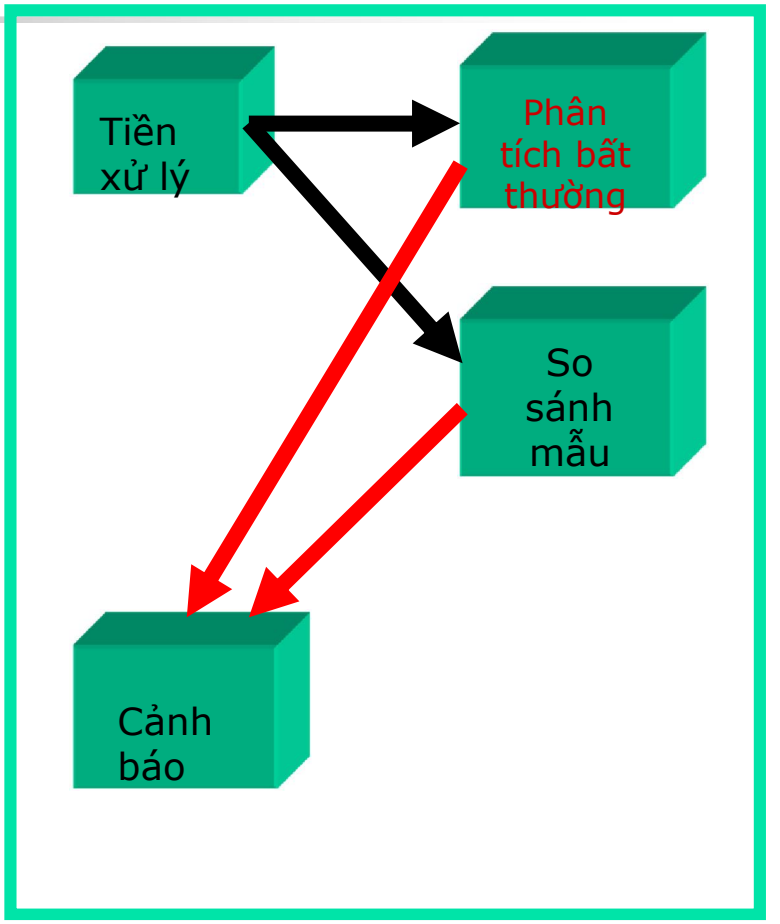
Modul phân tích phát hiện tấn công

- ***Phát hiện tình trạng bất thường (Anomaly detection models):***
  - Ban đầu, chúng lu giữ các mô tả sơ l-ợc về các hoạt động bình thờng của hệ thống.
  - Các cuộc tấn công xâm nhập gây ra các hoạt động bất bình thờng và kỹ thuật này phát hiện ra các hoạt động bất bình thờng đó.
    - Phát hiện dựa trên mức ngỡng,
    - Phát hiện nhờ quá trình tự học,
    - Phát hiện dựa trên những bất th-ờng về giao thức)



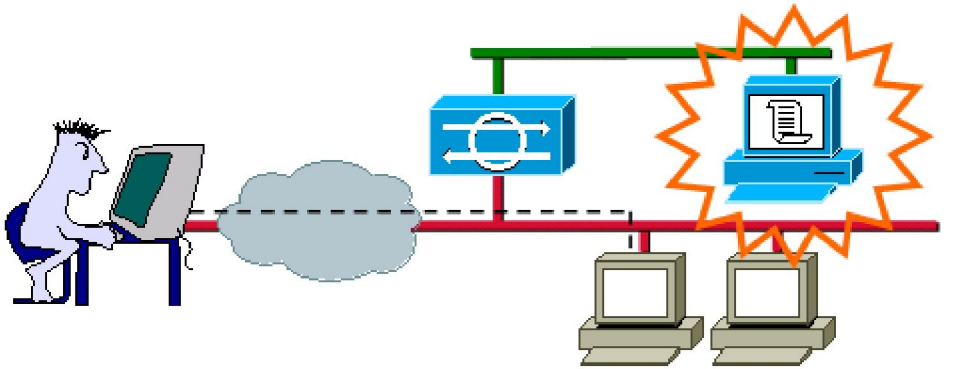
Modul phân tích phát hiện tấn công

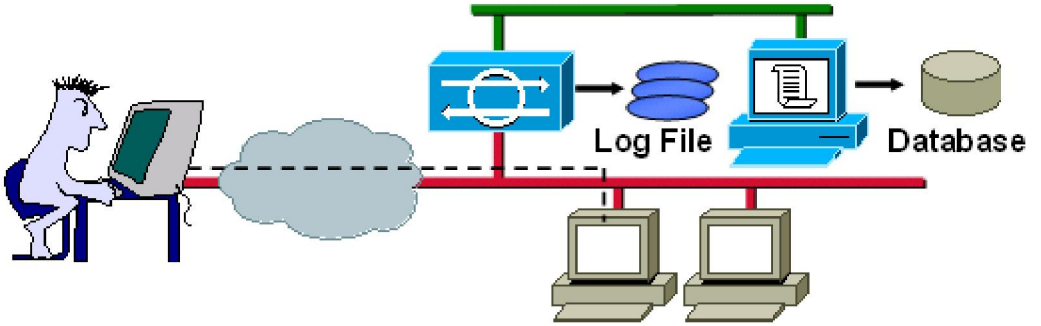
- ***Phát hiện tình trạng bất thường (Anomaly detection models):***
  - ***Ưu điểm:*** có thể phát hiện ra các kiểu tấn công mới, cung cấp các thông tin hữu ích bổ sung cho phương pháp dò sự lạm dụng
  - ***Nhược điểm:*** thường tạo ra một số lượng các cảnh báo sai làm giảm hiệu suất hoạt động của mạng.



Modul phân tích phát hiện tấn công

- ***Cảnh báo:*** Quá trình này thực hiện sinh ra các cảnh báo tùy theo đặc điểm và loại tấn công, xâm nhập mà hệ thống phát hiện được.





Modul phản ứng

- Khi có dấu hiệu của sự tấn công hoặc thâm nhập, modul phát hiện tấn công sẽ gửi tín hiệu báo hiệu có sự tấn công hoặc thâm nhập đến modul phản ứng.
- Modul phản ứng gửi tín hiệu kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị.

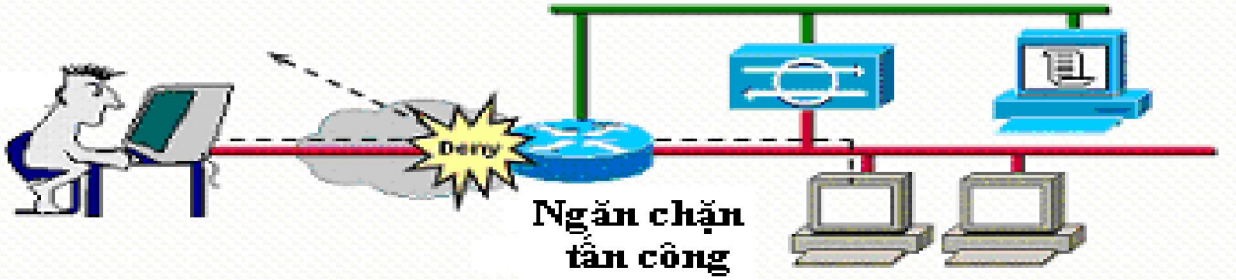
Modul phản ứng

TCP Reset

Tự động huỷ bỏ phiên làm việc

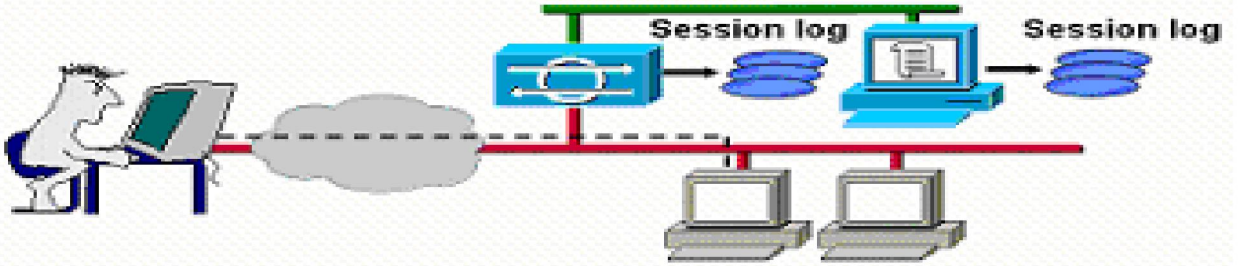
Ngăn chặn

Chặn địa chỉ IP của kẻ tấn công



Ghi chép

Ghi lại các hoạt động nghi ngờ



Xin chân thành cảm ơn!