CHƯƠNG VIII
PHÁT HIỆN THÂM NHẬP BẤT HỢP PHÁP

ThS. Nguyễn Cao Đạt
E-mail: dat@hcmut.edu.vn

Tham khảo

[1]. Cryptography and Network Security: chương 18

[2]. Network Security – A Beginner's Guide: module 13

Nội dung trình bày

- Khái niệm về thâm nhập bất hợp pháp
- Phát hiện thâm nhập bất hợp pháp là gì ?
- Phân loại các hệ thống phát hiện thâm nhập bất hợp pháp
- Khởi tạo và quản lý hệ thống phát hiện thâm nhập bất hợp pháp
- Lựa chọn hệ thống phát hiện thâm nhập bất hợp pháp để triển khai
- Hiểu biết về ngăn chặn thâm nhập bất hợp pháp

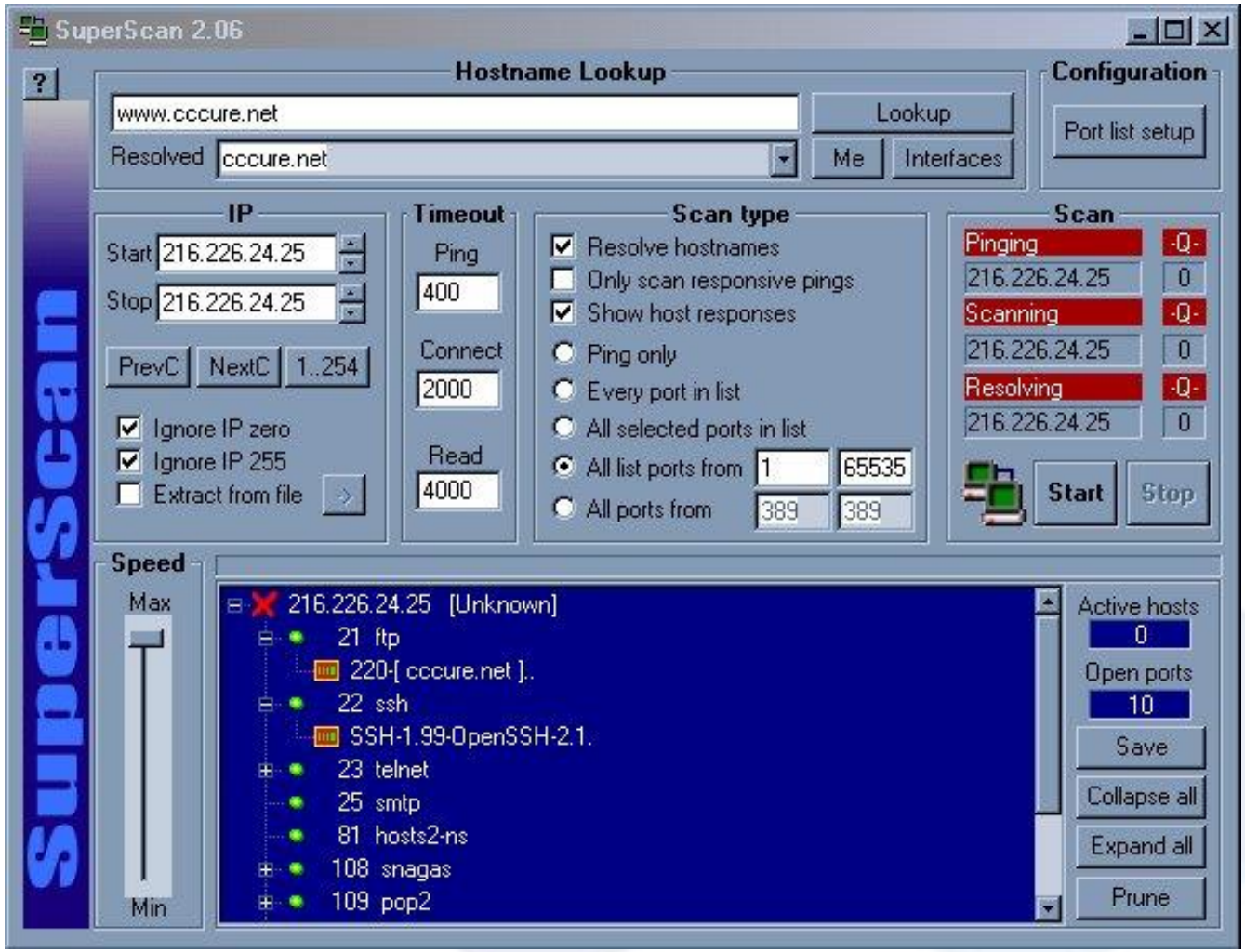
Khái niệm về thâm nhập bất hợp pháp

- Là các cố gắng truy cập hệ thống hay thao tác thông tin không được phép khiến chúng không đáng tin cậy hoặc không sử dụng được.
- **Phân loại**
  - Thâm nhập bất hợp pháp từ bên ngoài đến một số hệ thống máy tính bên trong
  - Thâm nhập bất hợp pháp từ người dùng hợp pháp đến dữ liệu, các chương trình, tài nguyên không được cấp quyền
  - Thâm nhập bất hợp pháp từ người kiểm soát hệ thống và sử dụng quyền này để né tránh hay ngăn chặn hệ thống kiểm soát truy cập và kiểm toán

Ví dụ thâm nhập bất hợp pháp

- **Quét địa chỉ IP**
  - Quét một vùng địa chỉ để tìm ra các máy chủ
- **Quét port**
  - Quét các cổng đang mở(ví dụ: 80/tcp, 21/tcp, …)
- **Đánh giá dịch vụ**
  - Xác định hệ điều hành, các phần mềm triển khai dịch vụ
- **Lựa chọn mục tiêu**
  - Lấy ra máy chủ dễ bị tổn thương nhất
- **Khai thác hệ thống, dò tìm các lỗ hổng**
  - Tấn công mật khẩu tự động trên các dịch vụ như FTP, HTTP, NetBIOS, VNC PCAnywhere….
  - Tấn công trên ứng dụng, dịch vụ cụ thể

Ví dụ thâm nhập bất hợp pháp



Các cách khai thác hệ thống

- Virus/Trojan/worm backdoor
- Từ chối dịch vụ
- Khai thác các Active Script
- Điểm yếu các giao thức
- Mật khẩu không an toàn
- Tràn bộ đệm buffer overflow
- Lỗi(bug) trong các ứng dụng, dịch vụ

Phát hiện thâm nhập bất hợp pháp

- Phát hiện các thâm nhập bất hợp pháp hoặc các nỗ lực thâm nhập bất hợp pháp bằng tay hay thông qua hệ thống chuyên gia phần mềm hoạt động các tập tin nhật ký hoặc các thông tin khác có sẵn trên hệ thống hoặc trên mạng.

Phát hiện thâm nhập bất hợp pháp

- **Lợi ích**
  - Ngăn chặn truy cập và thao tác trái phép và giảm thiểu thiệt hại nếu phát hiện nhanh chóng.
  - Hệ thống phát hiện xâm nhập hiệu quả có thể phục vụ như một bộ ngăn chặn.
  - Thu thập thông tin để cải thiện an ninh trong tương lai.

Phát hiện thâm nhập bất hợp pháp

- **Làm thế nào để phát hiện**
  - Giả sử rằng thâm nhập bất hợp pháp có hành vi khác so với người dùng hợp pháp
  - Sẽ không có sự phân biệt hoàn hảo

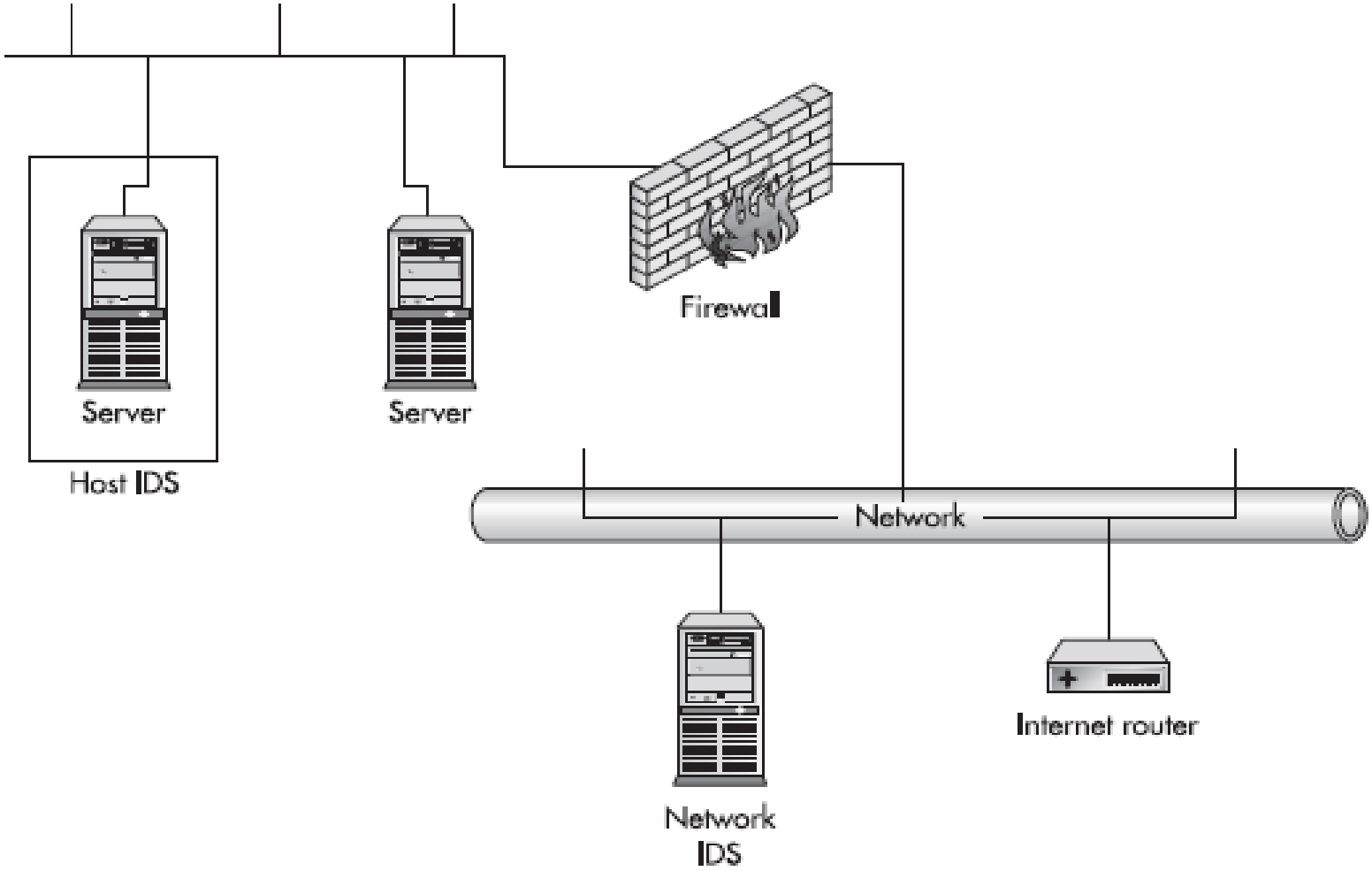
Các hướng tiếp cận

- **Phát hiện dựa trên thống kê**
  - Dựa trên ngưỡng
  - Dựa trên profile người dùng
- **Phát hiện dựa trên quy tắc**
  - Như thế nào là bất thường
  - Hệ chuyên gia được dùng để xác định quy tắc
- **Vấn đề cần xem xét**
  - Tăng cảnh báo đúng
  - Giảm cảnh báo giả

Phân loại IDS

- **HIDS** deep
  - Host-based Intrusion Detection System - hệ thống phát hiện thâm nhập bất hợp pháp trên máy chủ
  - Cài đặt trên máy chủ tìm kiếm dấu hiệu của các cuộc thâm nhập bất hợp pháp trên máy chủ đó
- **NIDS** breadth
  - Network-based Intrusion Detection System - Hệ thống phát hiện thâm nhập bất hợp pháp trên mạng
  - Cài đặt trên một hệ thống xem xét được thông tin liên lạc trên một mạng và tìm kiếm dấu hiệu của các cuộc thâm nhập bất hợp pháp trên mạng đó

Phân loại IDS



HIDS

- Một hệ thống các cảm biến được cài đặt trên một máy tính. Chúng xem xét các sự kiện và tạo ra các cảnh báo
- Lựa chọn tập cảm biến thích hợp cho mỗi máy chủ
- Các loại cảm biến bao gồm
  - Phân tích các tập tin nhật ký
  - Các cảm biến dựa trên dấu hiệu(signature)
  - Phân tích lời gọi hệ thống
  - Phân tích hành vi ứng dụng
  - Kiểm tra tính toàn vẹn hệ thống tập tin

Ưu điểm của HIDS

- Theo dõi ai đang truy cập những gì
- Có thể ánh xạ các hành động có vấn đề đến người dùng cụ thể
- Có thể theo dõi những thay đổi hành vi kết hợp với sử dụng sai mục đích
- Có thể hoạt động trong môi trường mã hóa dữ liệu https
- Hoạt động được trong mạng dùng chuyển mạch
- Giám sát phân bố, báo cáo dữ liệu liên quan đến giao diện điều khiển trung tâm

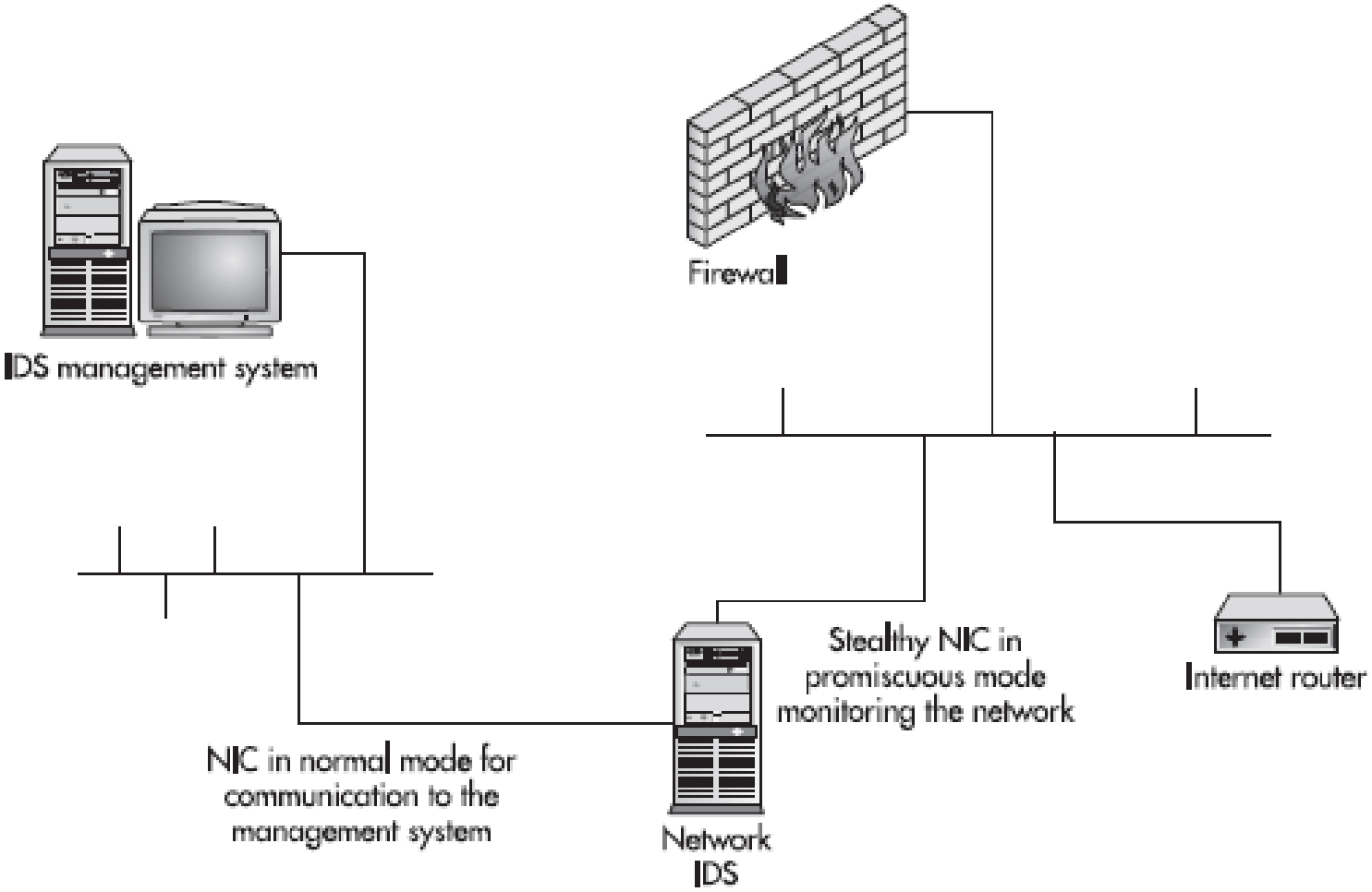
Nhược điểm của HIDS

- Không thể thấy tất cả hoạt động của mạng
- Hiệu suất có thể là một vấn đề. Ví dụ thực thi cơ chế kiểm toán có thể gây ra tình trạng quá tải cho hệ thống
- Mất nhiều dung lượng để lưu trữ các dấu vết kiểm toán
- Hệ điều hành có lỗ hổng có thể làm giảm độ hiệu quả HIDS
- Chi phí triển khai và bảo trì cao

NIDS

- Một hệ thống mà giao tiếp mạng được xét ở chế độ "promiscuous"
- Thu thập toàn bộ thông tin liên lạc trên mạng, chúng được phân tích dựa trên một tập các quy tắc và các dấu hiệu để xác định thông tin nào đáng quan tâm vào tạo các cảnh báo
- Tại thời điểm này, NIDS dựa chủ yếu trên các dấu hiệu

NIDS


Firewall
IDS management system
Stealthy NIC in promiscuous mode monitoring the network
Internet router
NIC in normal mode for communication to the management system
Network IDS

Ưu điểm của NIDS

- Có thể hoàn toàn ẩn trên mạng.
- Được sử dụng để theo dõi và phát hiện thời gian thực các tấn công trên một số lượng lớn các hệ thống.
- Có thể nắm bắt được nội dung của tất cả các gói dữ liệu đi và đến một hệ thống mà không cần cấu hình lại các hệ thống hay chuyển hướng các cơ chế ghi nhật ký.
- Không ảnh hưởng đến mạng và nguồn dữ liệu.
- Không tạo thêm chi phí trên các hệ thống.

Nhược điểm của NIDS

- Chỉ cảnh báo nếu trùng với các quy tắc hay các dấu hiệu đã cấu hình.
- Bỏ qua một số thông tin trên mạng nếu băng thông mạng cao.
- Không thể kiểm tra thông tin nếu thông tin được mã hóa.
- Khi mạng sử dụng chuyển mạch, ta cần cấu hình đặc biệt để NIDS có thể lấy được toàn bộ thông tin liên lạc trên mạng.

Khởi tạo và quản lý IDS

- **Khởi tạo IDS**
  - Như với hầu hết các hệ thống phức tạp, chính sách phải được tạo ra, xác nhận, và thử nghiệm trước khi triển khai.
- **Các bước để khởi tạo**
  - Xác định mục tiêu
  - Chọn thành phần, hệ thống để theo dõi
  - Chọn đáp ứng thích hợp
  - Xét các ngưỡng
  - Hiện thực chính sách

Khởi tạo và quản lý IDS

- **Quản lý IDS**
  - Cần có nhân sự 24/7 nếu mục tiêu của IDS là theo dõi tất cả các thâm nhập bất hợp pháp.
  - Khi có thâm nhập bất hợp pháp thì sẽ xử lý như thế nào ?
- **Các loại sự kiện**
  - Thăm dò
    - Thu thập thông tin một hay nhiều hệ thống trước khi tấn công thật sự.
    - Quét port, dịch vụ, lỗ hỗng, xem xét các tập tin.

Khởi tạo và quản lý IDS

- **Các loại sự kiện**
  - Thăm dò
  - Tấn công
    - Xác định độ ưu tiên các sự kiện.
    - Đánh giá các sự kiện(độ ưu tiên, số lượng) để xác định đó là một cuộc tấn công thật sự hay không.
  - Các vi phạm chính sách
    - Chia sẻ trên mạng ngang hàng(Gnutella, Kazaa, ..)
    - Instant messenger(Yahoo, ..)
    - Kết nối không an toàn: telnet, rlogin, rsh, ..

Khởi tạo và quản lý IDS

- **Các loại sự kiện**
  - Các sự kiện nghi ngờ hoặc không giải thích được
    - Thực hiện các bước cần thiết để xác định đó là hành vi bình thường hay là cố gắng thâm nhập bất hợp pháp
    - Các bước này bao gồm
      - Xác định các hệ thống liên quan.
      - Ghi nhận lưu lượng bổ sung giữa nguồn và đích.
      - Ghi nhận toàn bộ lưu lượng từ nguồn.
      - Ghi nhận nội dung các gói tin từ nguồn.

Lựa chọn IDS để triển khai

- **Các tính năng cần lưu ý**
  - Số lượng quy tắc, quy tắc nào sẽ được dùng trong môi trường mạng cụ thể của bạn
  - Khả năng đọc toàn bộ thông tin gói, khả năng đi sâu
  - Giải quyết đầy đủ với các phân mảnh
  - Cập nhật (thực hiện như thế nào và mức độ thường xuyên)
  - Vấn đề hỗ trợ hệ điều hành
  - Dễ sử dụng

on firewall

Lựa chọn IDS để triển khai

- **Các tính năng cần lưu ý**
  - Thiết bị chuyên dụng được yêu cầu là gì ?
  - Sản phẩm là NIDS hay HIDS
  - Chi phí triển khai và cập nhật
  - Nó có khả năng tự động phản ứng khi có tấn công hay không ?
  - Tỷ lệ các cảnh báo giả
  - Những kỹ năng cần thiết để hỗ trợ nó

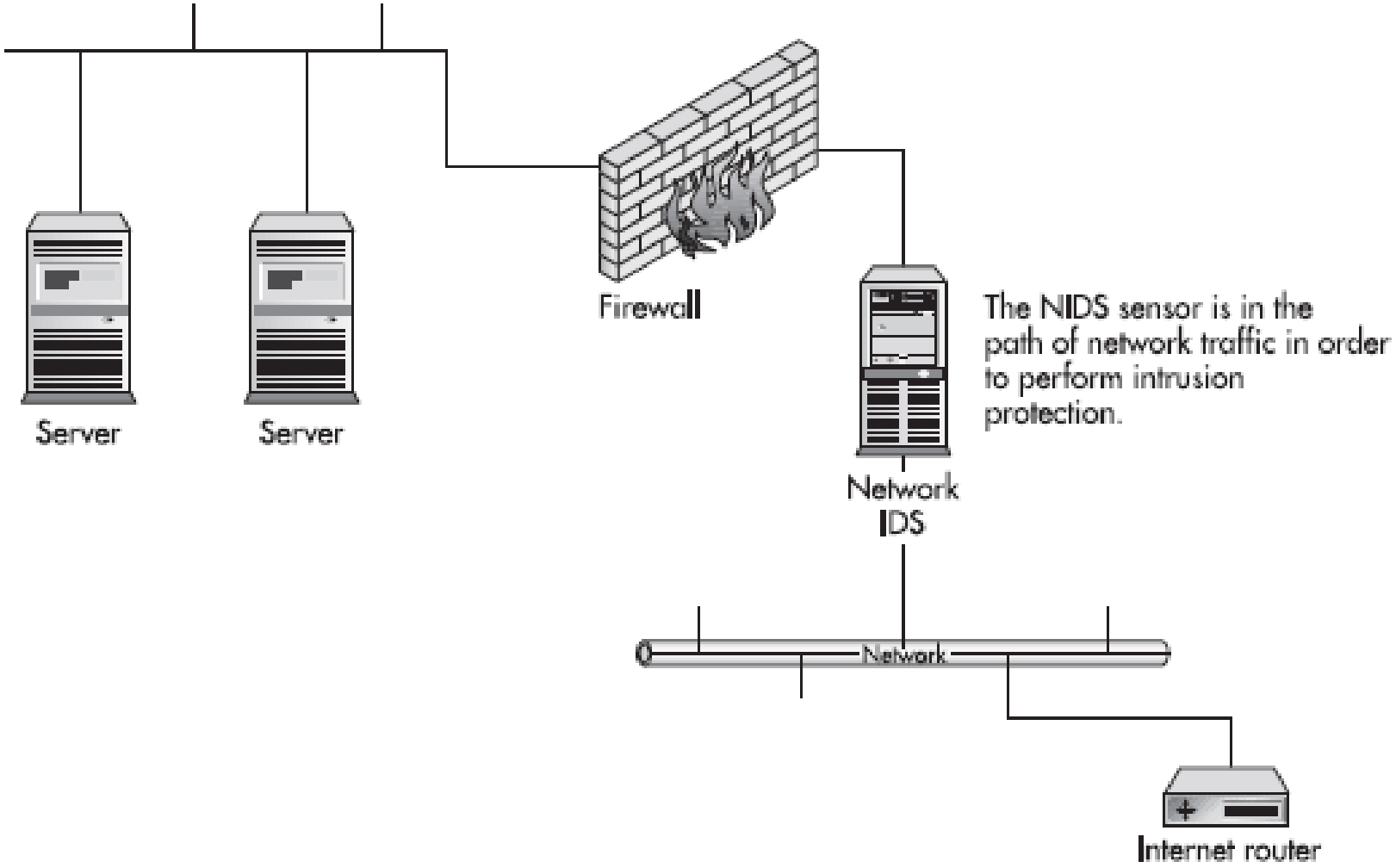
Lựa chọn IDS để triển khai

- **Các sản phẩm nổi trội**
- **Dragon của Enterasys**
  - http://www.enterasys.com/ids/
- **Secure IDS của Cisco**
  - http://www.cisco.com/go/ids/
- **Snort**
  - http://www.snort.org/
- **Real Secure của ISS**
  - http://www.iss.net/securing_e-business/
- **SHADOW**
  - http://www.whitehats.ca
  - ftp://ftp.whitehats.ca/pub/ids/shadow-slack/shadow.iso

Ngăn chặn thâm nhập bất hợp pháp

- Tâm điểm của các sản phẩm mới trong lĩnh vực phát hiện thâm nhập bất hợp pháp.
- IDS chủ động ngăn chặn thâm nhập bất hợp pháp ngay khi chúng diễn ra.
- Tức là phải dừng lại trước khi nó đạt đến hệ thống đích hoặc dừng lại trước khi hệ thống mục tiêu thực hiện mã khai thác lỗ hổng.
- Cơ chế thực hiện
  - Khá đơn giản đối với HIDS
  - Kiến trúc NIDS phải thay đổi để các cảm biến được đặt ngay trên dòng dữ liệu(như bức tường lửa).

Ngăn chặn thâm nhập bất hợp pháp



Ngăn chặn thâm nhập bất hợp pháp

- **Các vấn đề nảy sinh đối với ngăn chặn thâm nhập bất hợp pháp**
  - Từ chối dịch vụ
    - IDS có thể ngăn chặn một hành động hợp pháp. Điều này có nghĩa IDS gây ra từ chối dịch vụ.
    - Nếu IDS xác định không chính xác, tình trạng từ chối dịch vụ sẽ tiếp tục.
  - Sẵn sàng
    - Các cảm biến trên NIDS phải đáp ứng các yêu cầu sẵn sàng cao của các thành phần mạng khác.
    - Các cảm biến trên HIDS phải có tính sẵn sàng cao.

Tóm tắt

- Thâm nhập bất hợp pháp vào hệ thống máy tính hoặc mạng máy tính là một trong những mối đe dọa nghiêm trọng nhất đối với an ninh thông tin.
- Phát hiện thâm nhập bất hợp pháp liên quan đến việc phát hiện các kiểu hoạt động hay mô hình hoạt động được biết là tương quan với sự thâm nhập bất thường.
- Hệ thống phát hiện thâm nhập bất hợp pháp được triển khai nhằm cung cấp cảnh báo sớm của một thâm nhập bất hợp pháp để hành động phòng thủ được thực hiện để ngăn chặn hoặc giảm thiểu thiệt hại.
- Ngăn chặn thâm nhập bất hợp pháp có một số vấn đề.