ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

AN NINH MẠNG

Bài 12.

Một số hệ thống phòng chống tấn công mạng

1. Tường lửa (Firewall)

Giới thiệu chung

- Là hệ thống có khả năng ngăn chặn các truy cập không hợp lệ và **đã biết** từ bên ngoài và trong khu vực tài nguyên cần bảo vệ
- Tường lửa có thể triển khai ở nhiều vị trí, tùy thuộc cách thức định nghĩa, phạm vi tài nguyên cần bảo vệ:
  - Mạng ngoại vi
  - Mạng nội bộ

  } Network-based firewall
  - Nút mạng(Host-based firewall)
  - Ứng dụng(Application-based firewall)

Tường lửa có thể làm gì?

- Thi hành các chính sách an toàn bảo mật: hoạt động như một hệ thống cảnh vệ(traffic cop) cho phép/từ chối lưu lượng mạng nào đó **đi qua** tường lửa dựa trên các đặc điểm(giao thức, địa chỉ, nội dung…) **đã xác định**
- Hạn chế các hành vi tấn công vào mạng
  - Từ mạng bên ngoài(Internet) vào mạng nội bộ
  - Từ phân vùng mạng nội bộ này tới những phân vùng mạng nội bộ khác
- Lưu nhật ký các lưu lượng mạng

Tường lửa không thể làm gì?

- Không bảo vệ được tài nguyên trước các mối nguy cơ từ bên trong
- Không kiểm soát được các lưu lượng mạng không đi qua
- Không kiểm soát đầy đủ đối với các lưu lượng đã được mã hóa
- Không ngăn chặn được các truy cập tấn công chưa biết
- Không chống lại được hoàn toàn các nguy cơ từ phần mềm độc hại
- Do đó cần được:
  - Triển khai ở nhiều vị trí khác nhau
  - Kết hợp với các giải pháp khác: phòng chống phần mềm độc hại, IDS/IPS, điều khiển truy cập, kiểm toán(auditing)
  - Cập nhật liên tục các chính sách mới

Các kiến trúc tường lửa(1)

- Network-based firewall: Kiểm soát lưu lượng mạng giữa các phân vùng mạng
- Ưu điểm: Phạm vi kiểm soát rộng
- Nhược điểm:
  - Không kiểm soát được lưu lượng trong từng phân vùng
  - Không kiểm soát đầy đủ lưu lượng đã được mã hóa

Các kiến trúc tường lửa(2)

- Host-based firewall: Kiểm soát lưu lượng mạng đến và đi từ một nút mạng
- Ưu điểm: Kiểm soát được lưu lượng tới nút mạng từ những nguồn trong cùng phân vùng mạng
- Nhược điểm:
  - Chỉ bảo vệ được cho một mục tiêu đơn lẻ
  - Không kiểm soát đầy đủ lưu lượng đã được mã hóa

Các kiến trúc tường lửa(3)

- Application firewall: Kiểm soát lưu lượng mạng của một dịch vụ cụ thể
- Ưu điểm: Kiểm soát được toàn bộ lưu lượng mạng tới dịch vụ, kể cả lưu lượng đã mã hóa
- Nhược điểm:
  - Bộ luật phức tạp
  - Cần phải cài đặt nhiều phần mềm tường lửa nếu trên máy chủ cung cấp các dịch vụ khác nhau

Các thế hệ tường lửa

- Thế hệ 1(1985) – Packet filter: kiểm soát lưu lượng dựa trên các thông tin trong phần tiêu đề
- Thế hệ 2(1989) – Proxy server: có thể ngăn chặn lưu lượng tấn công dựa trên sự hiểu biết về các giao thức chuẩn của tầng ứng dụng
- Thế hệ 3(1991) – Stateful inspector firewall: kiểm soát thêm trạng thái của luồng dữ liệu
- Thế hệ 4(1994) – Dynamic packet filter: giao tiếp với hệ thống phát hiện tấn công để cung cấp các cơ chế phản ứng với tấn công
- Thế hệ 5(1996) – Kiểm soát quá trình xử lý gói tin dựa trên toàn bộ chồng giao thức TCP/IP
- Hiện nay: tích hợp với các giải pháp an toàn bảo mật khác

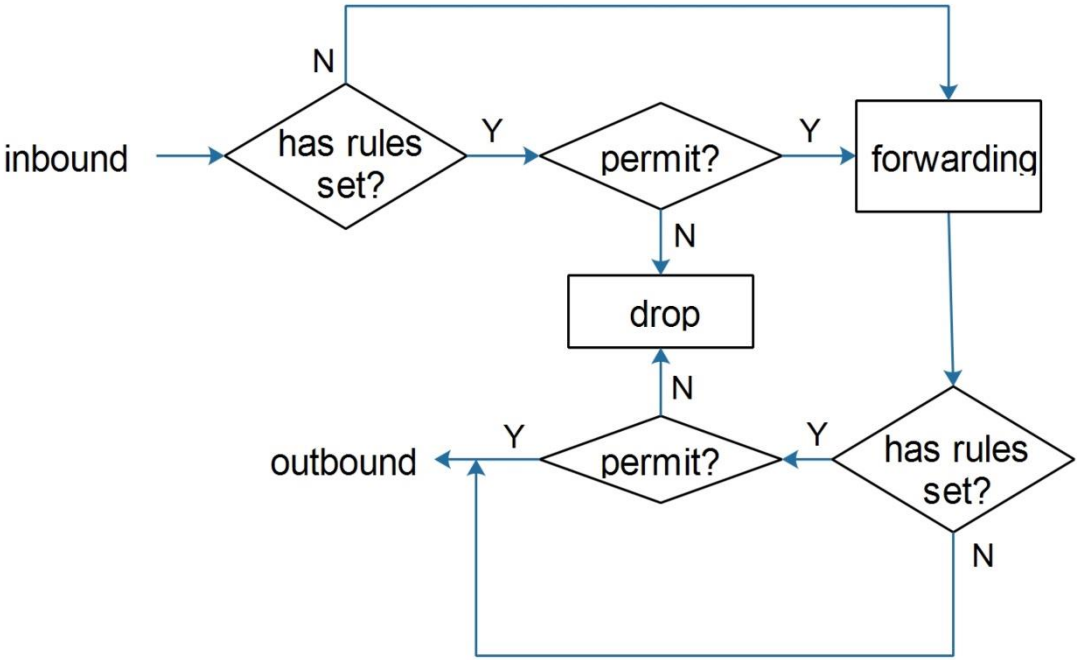
Packet filter(stateless)

- Loại tường lửa đơn giản nhất
- Dựa trên việc kiểm tra một số giá trị trong phần tiêu đề để xác định gói tin được chấp nhận hoặc chặn:
  - Địa chỉ MAC
  - Địa chỉ IP nguồn, đích
  - Số hiệu cổng nguồn, đích
  - Giao thức
- Ví dụ:

Rule	Source IP	Source port	Destination IP	Destination port	Action
1	Any	Any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	Any	Any	Any	Deny
3	Any	Any	192.168.120.1	Any	Deny
4	192.168.120.0	Any	Any	Any	Allow
5	Any	Any	192.168.120.2	25	Allow
6	Any	Any	192.168.120.3	80	Allow
7	Any	Any	Any	Any	Deny

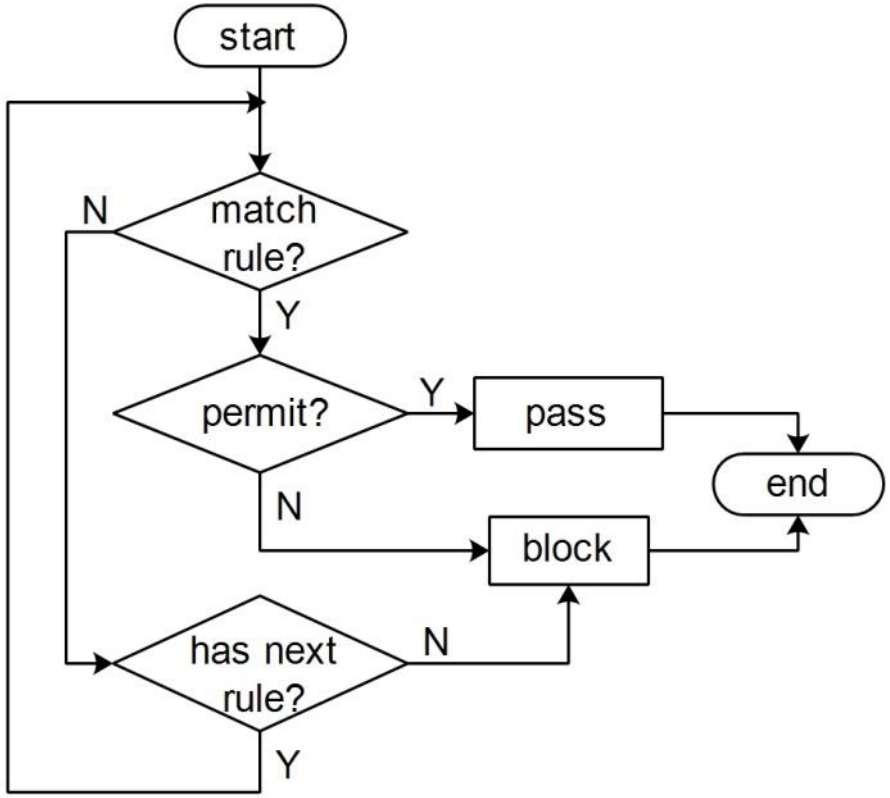
Packet filter – Nguyên lý hoạt động

- Mỗi firewall có một tập các luật định nghĩa cách thức xử lý gói tin(cho phép đi qua hoặc chặn).
- Tập các luật có thể áp dụng trên luồng dữ liệu đi vào(inbound) hoặc đi ra(outbound) của giao tiếp mạng trên firewall



Packet filter – So khớp luật

- Thông tin trên phần tiêu đề của gói tin được so khớp với các giá trị định nghĩa trong luật
- Các luật được so khớp theo thứ tự sắp đặt trong tập luật
- Nếu phù hợp với luật nào, gói tin được xử lý theo cách thức đã chỉ ra trong luật đó
  - Không tiếp tục so khớp với các luật còn lại
- Nếu không có luật nào được so khớp: xử lý theo luật mặc định
  - Thông thường: luật mặc định là chặn



Packet filter(stateless)

- Ưu điểm:
  - Đơn giản
  - Tốc độ xử lý nhanh
- Hạn chế:
  - Có quá ít lựa chọn xử lý(drop, accept, forward)
  - Không kiểm soát được nội dung gói tin
  - Khả năng hỗ trợ ghi nhật ký hạn chế
  - Dễ dàng vượt qua bằng các kỹ thuật giả mạo thông tin trên phần tiêu đề
  - Không hỗ trợ tính năng xác thực

Stateful Inspector/Filter

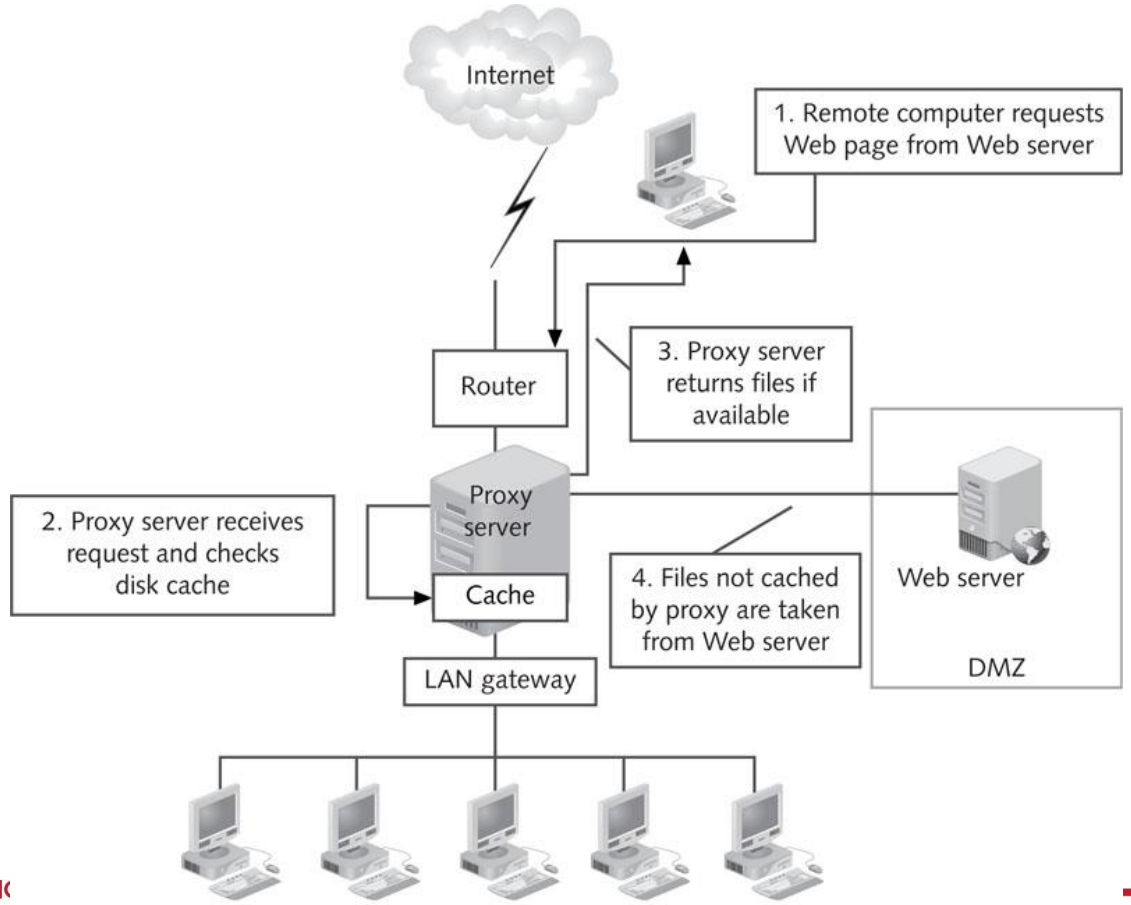
- Hạn chế của Packet filter: chỉ xử lý độc lập từng gói tin, không có cơ chế theo dõi trạng thái của liên kết
  - Ví dụ: Cho phép các gói tin từ External network vào Internal network nếu nút mạng trong Internal network đã khởi tạo liên kết
- Stateful Inspector
  - Sử dụng bảng lưu thông tin trạng thái của các liên kết đã được thiết lập
  - Cho phép dữ liệu đi vào(inbound) trong khu vực tài nguyên được bảo vệ khi và chỉ khi liên kết đã được thiết lập
  - Vẫn hỗ trợ các giao thức hướng không liên kết: chỉ cho phép dữ liệu đi vào nếu trước đó đã có dữ liệu đi ra tương ứng

Dynamic Packet filter

- Static packet filter: tập luật do người quản trị cấu hình
  - Luôn cần cập nhật thường xuyên
  - Không phản ứng kịp thời nếu tài nguyên bị tấn công
- Dynamic packet filter: luật được cập nhật tự động nếu có bất thường, tấn công xảy ra:
  - Thường kết hợp với các hệ thống IDS
  - Tạo cơ chế phản ứng với sự cố, bất thường trong mạng
  - Ví dụ: chặn tất cả các dữ liệu từ địa chỉ IP có số lượng gói tin lỗi vượt quá ngưỡng nào đó

Proxy server

- Tường lửa hoạt động ở tầng ứng dụng
- Chuyển tiếp dữ liệu đến và đi ra khỏi mạng
- VD: Web proxy



Proxy server – Ưu điểm

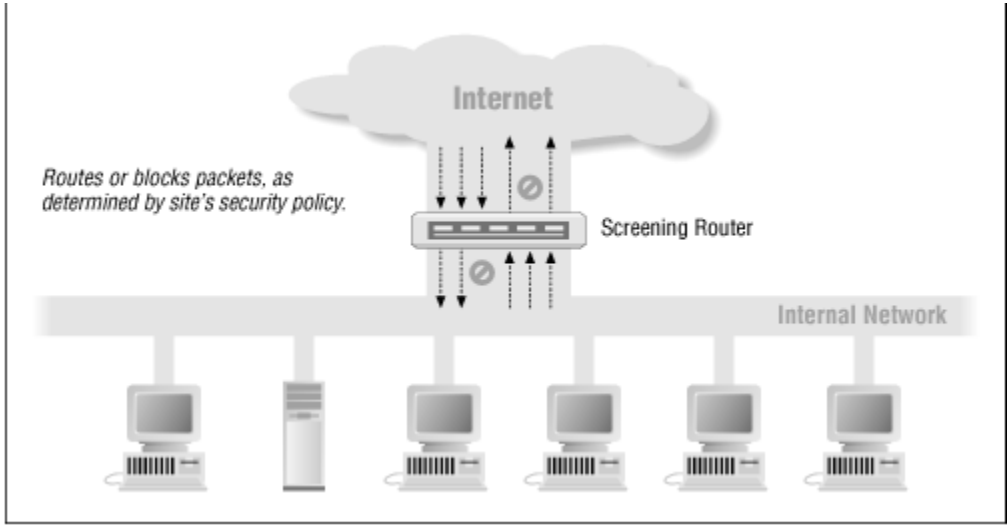
- Kiểm soát được nội dung của dữ liệu: URL filtering, MIME filtering, Content filtering
- Kiểm soát được trạng thái của phiên
- Che giấu được địa chỉ IP riêng
- Tách thông tin tiêu đề cũ, thay thế bằng tiêu đề mới → ngăn chặn các kỹ thuật tấn công dựa trên tiêu đề của gói tin tới mạng bên trong
- Chống lại việc giả mạo thông tin của tiêu đề
- Có thể định tuyến cho dịch vụ
- Hỗ trợ tốt các cơ chế nhật ký, kiểm toán

Proxy server – Hạn chế

- Làm chậm quá trình cung cấp dịch vụ
- Các dịch vụ hỗ trợ bị hạn chế
- Không trong suốt với người dùng cuối:
  - Cần cấu hình để client kết nối tới proxy server
- Hiện nay proxy server có thể thay thế bằng các sản phẩm tường lửa có tính năng Deep Packet Inspection

Screening router

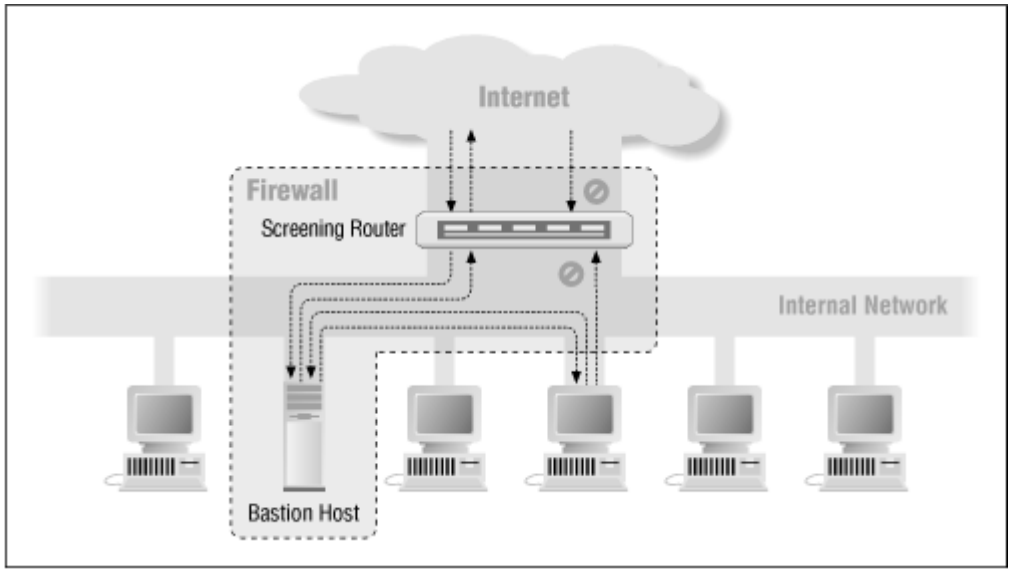
- Tích hợp bộ lọc với trên router kết nối mạng cần bảo vệ với mạng công cộng
- Ưu điểm:
  - Đơn giản
  - Chi phí thấp
- Nhược điểm:
  - Không có khả năng chịu lỗi
  - Mức độ an ninh thấp, dễ bị vượt qua



- Sử dụng khi nào?
  - Hệ thống đã có các lớp bảo vệ an toàn hơn ở bên trong
  - Số lượng giao thức cần kiểm soát ít

Screened-host

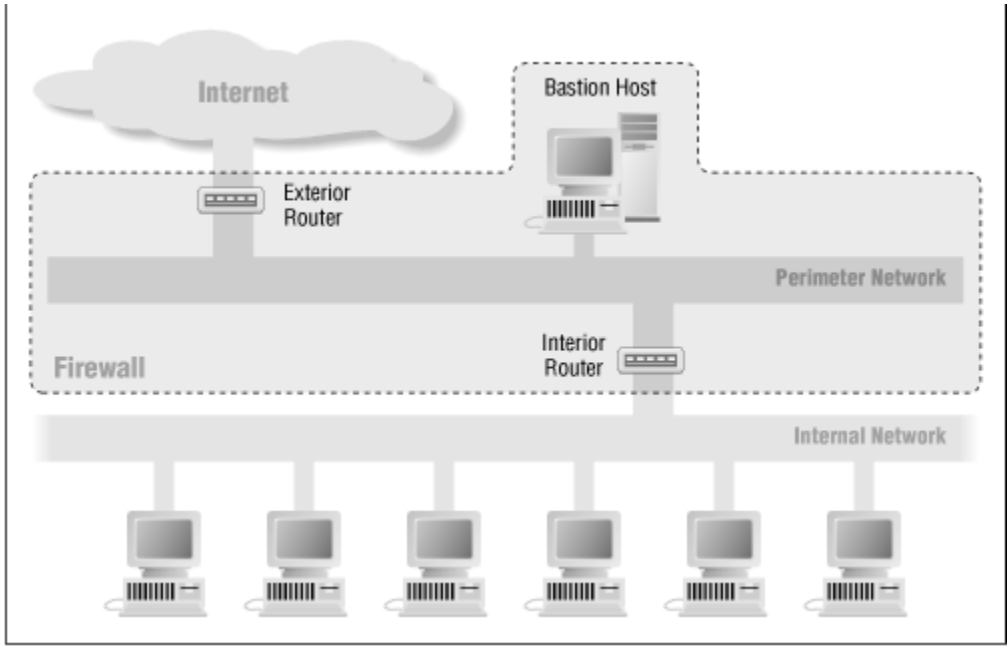
- Bastion Host đặt trên phân vùng mạng bên trong, là nút mạng duy nhất có thể truy cập từ mạng công cộng
- Bastion Host cần được bảo vệ ở mức cao nhất có thể
- Hạn chế: khi Bastion Host bị chiếm quyền quyền điều khiển, mạng bên trong không còn được bảo vệ



- Sử dụng khi nào?
  - Lưu lượng mạng thấp
  - Các nút của phân vùng mạng bên trong đã có lớp bảo vệ an toàn hơn

Screen-subnet

- Perimeter network: Phân vùng mạng vành đai nằm giữa phần vùng bên trong (internal network) và phần vùng bên ngoài (external network)
- Cài đặt packet filter trên cả 2 router
- Bastion Host có thể hoạt động như một proxy
- An toàn hơn do Bastion Host được tách biệt khỏi phân vùng bên trong

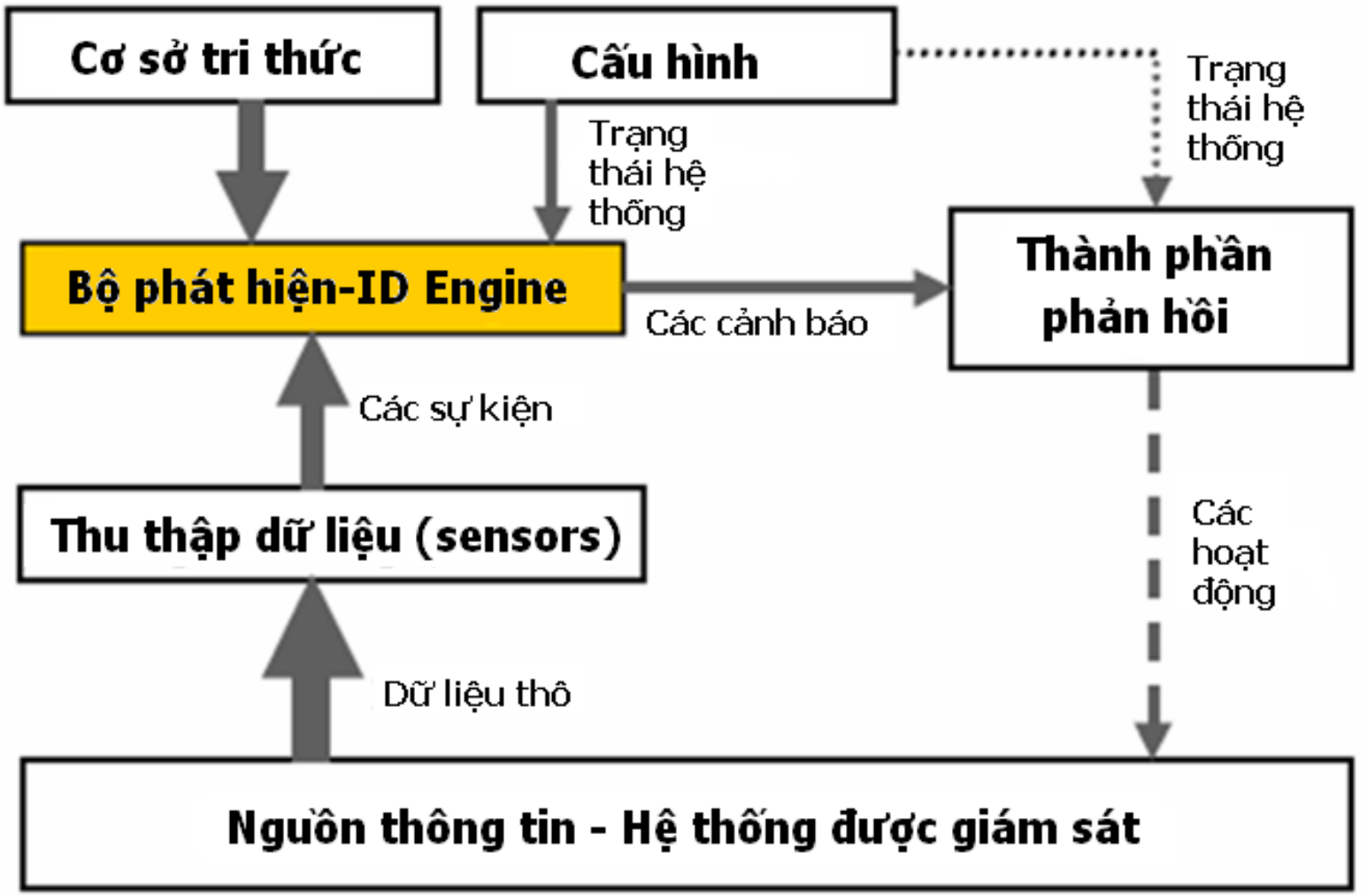


2. Hệ thống IDPS

Hệ thống IDPS

- Intrusion Detection and Preventation System: hệ thống có khả năng theo dõi, giám sát, phát hiện và ngăn chặn các hành vi tấn công, khai thác trái phép tài nguyên được bảo vệ
- Yêu cầu:
  - Tính chính xác
  - Tính kịp thời
  - Khả năng tự bảo vệ
- IDPS vs tường lửa:
  - Tường lửa: xử lý từng gói tin trên lưu lượng mạng
  - IDPS: có khả năng theo dõi, giám sát chuỗi các gói tin, hành vi để xác định có phải là hành vi tấn công hay xâm nhập hay không
  - Các thiết bị tường lửa thế hệ mới thường trang bị tính năng IDPS

Cấu trúc chung của IDPS



Cấu trúc chung của IDPS (tiếp)

- **Bộ cảm biến (Sensor):** thu thập dữ liệu từ hệ thống được giám sát.
- **Bộ phát hiện** : Thành phần này phân tích và tổng hợp thông tin từ dữ liệu thu được của bộ cảm biến dựa trên cơ sở tri thức của hệ thống
- **Bộ lưu trữ :** Lưu trữ tất cả dữ liệu của hệ thống IDS, bao gồm: dữ liệu của bộ cảm biến, dữ liệu phân tích của bộ phát hiện, cơ sở tri thức, cấu hình hệ thống … nhằm phục vụ quá trình hoạt động của hệ thống IDS.
- **Bộ phản ứng :** Thực hiện phản ứng lại với những hành động phát hiện được.
- **Giao diện người dùng**

Network-based IDPS (NIDPS)

- Chức năng: Thu thập và giám sát lưu lượng mạng dựa trên việc triển khai sensor tại nhiều điểm khác nhau trong mạng
  - Sensor có thể là các thiết bị có khả năng phân tích, tổng hợp và thống kê thông tin lưu lượng
  - Sensor phần mềm cài đặt trên một số nút mạng nhất định
- Các loại sensor sử dụng cho NIDPS:
  - Sensor nội tuyến(Inline sensor): đặt tại các vị trí mà lưu lượng mạng bắt buộc phải đi qua
  - Sensor thụ động (Passive sensor): có thể sao chép lưu lượng mạng → không bắt buộc lưu lượng mạng phải đi qua

NIDPS

- Ưu điểm:
  - Kiểm soát được toàn bộ hoặc phần lớn hệ thống mạng với yêu cầu số lượng ít các sensor cần triển khai
  - Trong hầu hết các trường hợp, NIDPS sensor hoạt động ở chế độ thụ động → ít gây ảnh hưởng tới hoạt động của mạng
  - Khó bị phát hiện bởi kẻ tấn công, chịu lỗi tốt
- Nhược điểm:
  - Lượng thông tin phải xử lý lớn
  - Không phân tích được các thông tin được mã mật
  - Tính chính xác thấp

Host-based IDPS (HIDPS)

- Chức năng: thu thập và phân tích thông tin để phát hiện tấn công trên nút mạng cụ thể:
  - Lưu lượng đến và đi
  - Trạng thái của hệ thống: các tiến trình, quản lý tài nguyên, truy cập file, log, thay đổi cấu hình…
  - Hoạt động và trạng thái của các ứng dụng
- Mô hình tập trung:
  - Sensor đặt trên các nút mạng để thu thập thông tin
  - HIDPS Server: phân tích thông tin do sensor thu thập và phát cảnh báo tới nút mạng
- Mô hình phân tán: sensor và HIDPS triển khai trên cùng nút mạng

HIDPS

- Ưu điểm:
  - Phân tích được các hành vi ngay trên mục tiêu → khó bị các kỹ thuật tấn công "qua mặt"
  - Kiểm soát toàn diện lưu lượng đến và đi
  - Chống lại các nguy cơ tấn công từ bên trong nút mạng(malware)
  - Thông tin phong phú từ log
- Hạn chế
  - Số lượng sensor tăng theo số lượng các nút cần giám sát
  - Có thể xuất hiện các lỗ hổng bảo mật từ chính HIDPS → tăng nguy cơ cho nút mạng
  - Khả năng tương tác với các HIDPS khác là hạn chế
  - Có thể làm giảm hiệu năng hoạt động của nút mạng

Phát hiện dựa trên dấu hiệu

- Attack Signature-based detection
- Sử dụng các thông tin **đã biết** về các kỹ thuật tấn công
  - Mã khai thác tấn công, giá trị đầu vào…
  - Nội dung của các gói tin…
- Ví dụ: Snort rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET (msg:"EXPLOIT
x86 linux samba overflow", flow: to_server,
established, content:"|eb2f 5feb 4a5e 89fb 893e
89f2|", reference: bugtraq, reference: CVE-1999-0811,
classtype: attempted-admin; sid:1497; rev:6)
```

- Nguồn thông tin tham khảo đặc trưng của các dạng tấn công: http://www.securityfocus.com/bid

Phát hiện dựa trên dấu hiệu

- Ưu điểm:
  - Triển khai đơn giản
  - Có thể chia sẻ CSDL về dấu hiệu của các dạng tấn công
  - Xác suất phát hiện nhầm thấp
- Hạn chế:
  - Chỉ phát hiện được các kỹ thuật tấn công đã biết
  - Cần cập nhật CSDL thường xuyên → kích thước CSDL tăng → giảm hiệu năng
  - Dấu hiệu xác định dựa trên cú pháp, thay vì dựa trên ngữ nghĩa → có thể bị vượt qua(bypass)

Phát hiện dựa trên lỗ hổng

- Vulnerability Signature-based detection
- Sử dụng các thông tin đặc trưng về dạng lỗ hổng đã biết

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-MISC cross site scripting attempt";
flow:to_server,established; content:"<SCRIPT>";
nocase; classtype:web-application-attack; sid:1497;
rev:6;)
```

- Cho phép phát hiện những tấn công cùng dạng
- Giảm kích thước CSDL dấu hiệu
- Hạn chế:
  - Có thể bị vượt qua
  - Không dễ để xác định dấu hiệu

Phát hiện dựa trên bất thường

- Anomaly-based detection
- Ý tưởng: Khi tấn công xảy ra, hệ thống xuất hiện những đặc điểm khác thường
- Thực hiện:
  - Xây dựng mô hình các hành vi, trạng thái khi hệ thống hoạt động bình thường
  - Phát hiện và đo lường các hành vi, trạng thái nằm ngoài mô hình
- Ưu điểm: có thể phát hiện được các dạng tấn công chưa biết

Phát hiện dựa trên bất thường

Phát hiện dựa trên ngưỡng(threshold-based)

- Thiết lập các giá trị giới hạn cho một số đặc điểm của hệ thống (CPU Usage, RAM usage, số kết nối…)
- Phát hiện tấn công nếu các giá trị quan sát được vượt ngưỡng
- Có thể phối hợp nhiều đặc điểm, ngưỡng

```
alert tcp !$HOME_NET any -> $HOME_NET 80 (flags: S;
msg:"Possible TCP DoS"; flow: stateless; threshold: type
both, track by_src, count 70, seconds 10;
sid:10001;rev:1;)
```

- Hạn chế: Độ chính xác thấp

Phát hiện dựa trên bất thường

Phát hiện dựa trên hành vi(Behavioral-based)

- Giám sát chuỗi các hành vi, hoạt động trên hệ thống
- Ví dụ:
  - Xác định chuỗi các lời gọi hệ thống phát sinh việc thực thi chương trình: **read**(), **open**(), **write**(), **fork**(), **exec**()…
  - Chuỗi các truy vấn SQL được thực hiện
- Ưu điểm: Độ chính xác cao
- Hạn chế:
  - Khó xây dựng mô hình, có thể gây bùng nổ tổ hợp với các hệ thống phức tạp
  - Có ít khả năng ngăn chặn

ĐẠI HỌC BÁCH KHOA

25 YEARS ANNIVERSARY SOICT

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thảo luận