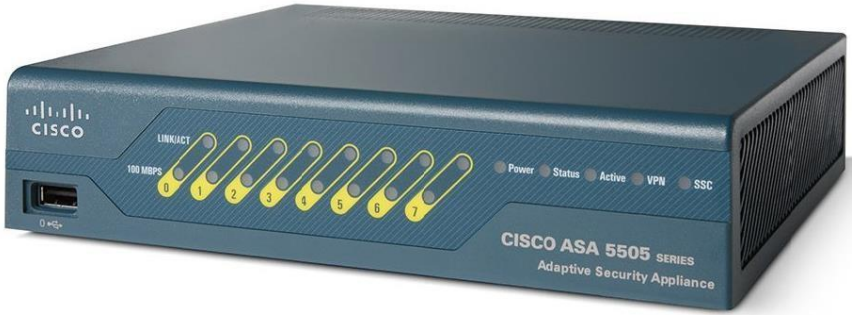
1. Tường lửa

1.1 Giới thiệu tường lửa

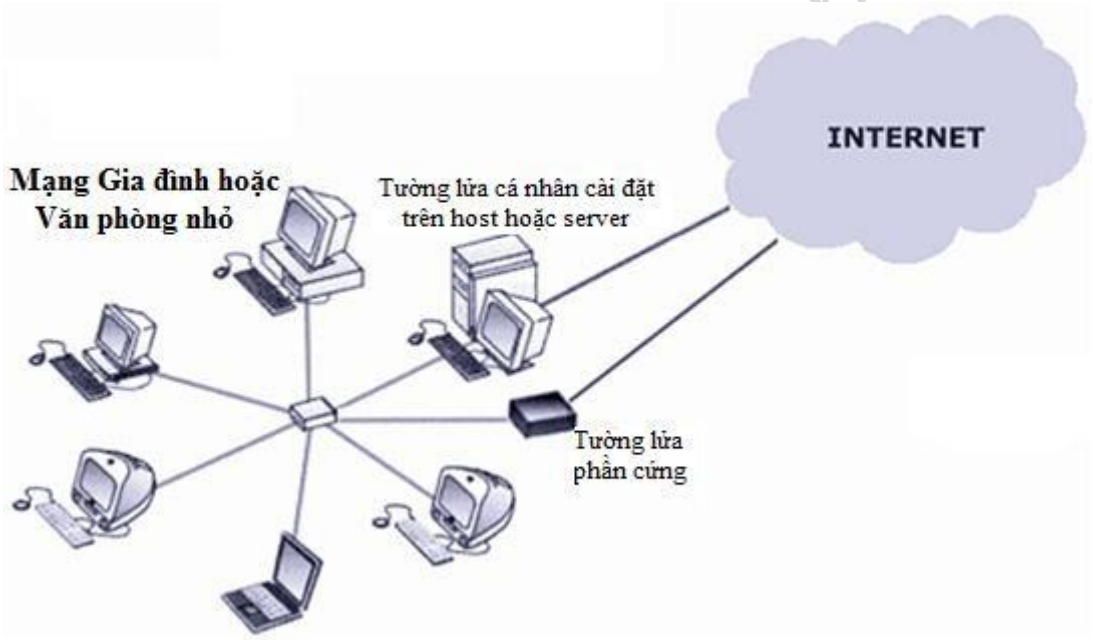
Tường lửa (Firewall) là một trong các kỹ thuật được sử dụng phổ biến nhất để bảo hệ thống và mạng cục bộ tránh các mối đe dọa từ bên ngoài. Tường lửa có thể là một thiết bị phần cứng chuyên dụng, hoặc mô đun phần mềm chạy trên máy tính. Hình 4.12 là hình ảnh một tường lửa phần cứng chuyên dụng của hãng Cisco.

Để đảm bảo hiệu quả bảo vệ, tường lửa phải miễn dịch với các loại tấn công, xâm nhập và thường được đặt ở vị trí cổng vào của mạng nội bộ cơ quan hoặc tổ chức, như minh họa trên Hình 4.13. Nhờ vị trí đặt ở cổng mạng, tất cả các gói tin từ trong ra và từ

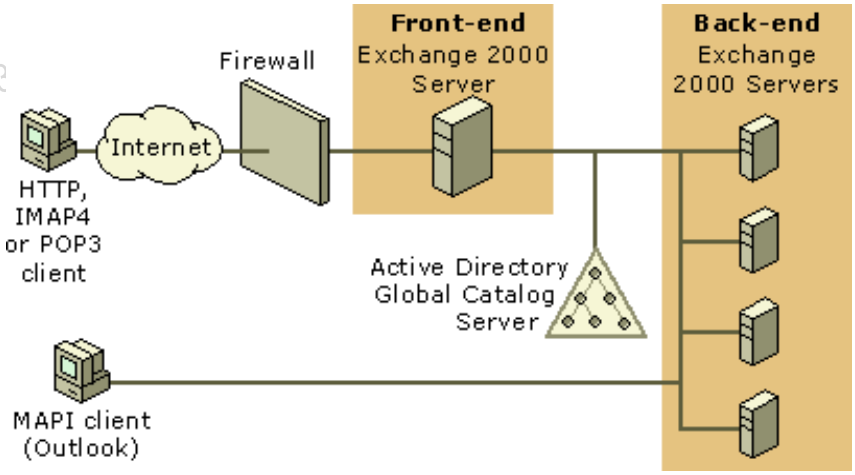
ngoài vào đều phải đi qua tường lửa và chỉ các gói tin hợp pháp được phép đi qua tường lửa. Việc xác định một gói tin là hợp pháp hay không được thực hiện bởi thao tác lọc (filtering) dựa trên các luật (rules). Tập các luật sử dụng cho việc lọc các gói tin được tạo ra dựa trên chính sách an ninh của cơ quan, tổ chức.



Hình 4.12. Một tường lửa phần cứng chuyên dụng của Cisco



Hình 4.13. Tường lửa bảo vệ mạng gia đình hoặc văn phòng nhỏ

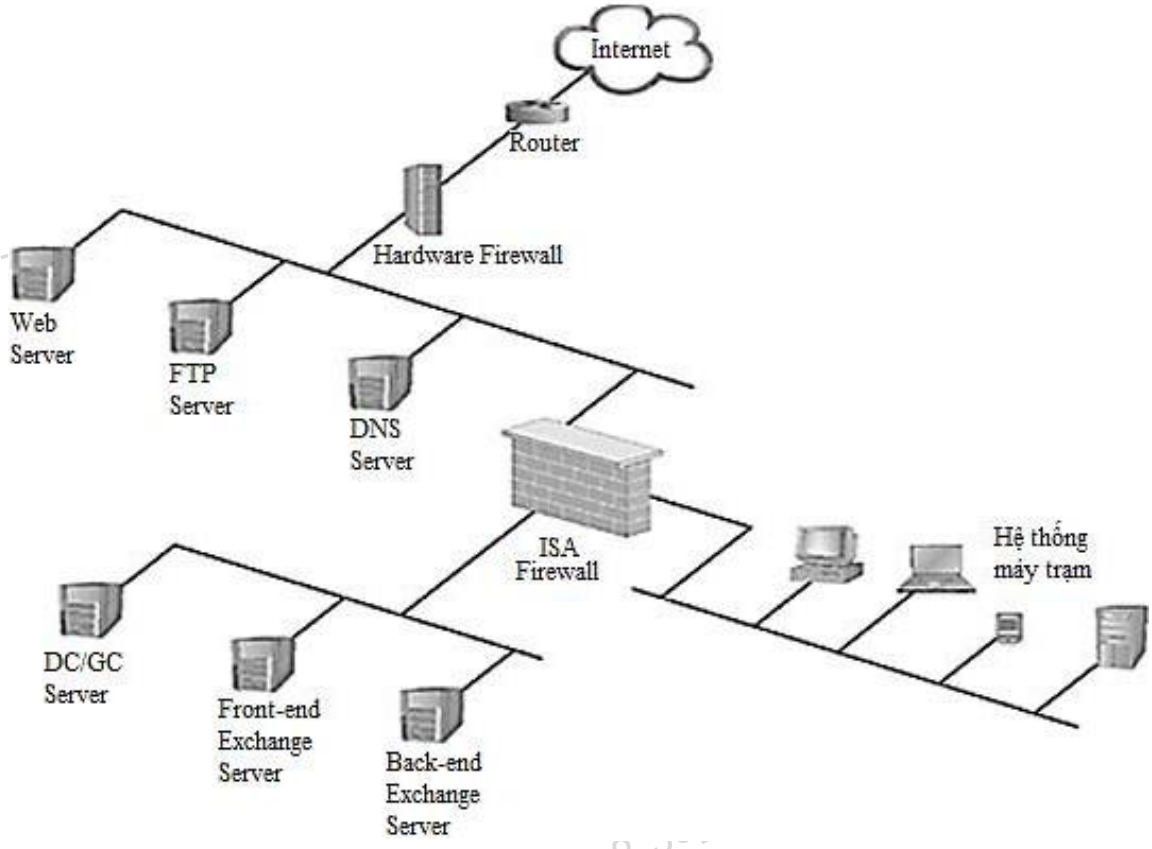


Hình 4.14. Tường lửa bảo vệ các máy chủ dịch vụ

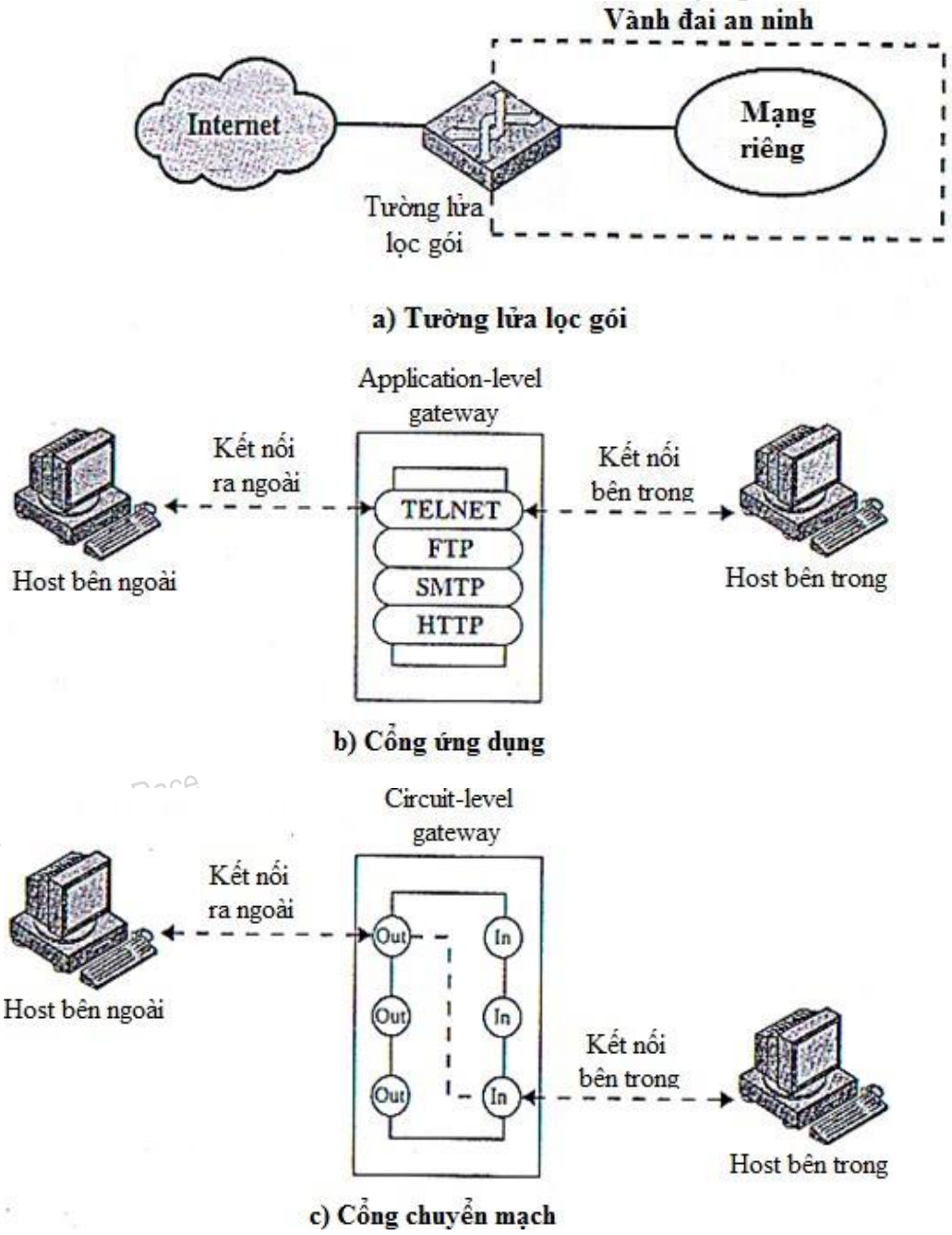
Hình 4.14 biểu diễn sơ đồ mạng trong đó tường lửa được sử dụng để bảo vệ các máy chủ dịch vụ email Microsoft Exchange. Tất cả các kết nối đến hệ thống máy chủ email đều phải đi qua tường lửa. Hình 4.15 sơ đồ mạng sử dụng 2 tường lửa để bảo vệ, trong đó một tường lửa phần cứng (Hardware Firewall) được sử dụng tại cổng kết nối Internet để bảo vệ các máy chủ dịch vụ (dịch vụ web, dịch vụ FTP và dịch vụ DNS) và một tường lửa phần mềm (ISA Firewall) được sử dụng để bảo vệ các máy chủ nội bộ và các máy trạm trong mạng LAN của cơ quan, tổ chức. Hai tường lửa có chính sách kiểm soát truy nhập và tập luật khác nhau phù hợp với đối tượng bảo vệ khác nhau.

1.2 Các loại tường lửa

Có nhiều phương pháp phân loại các tường lửa, chẳng hạn như dựa trên vị trí các lớp giao thức mạng và khả năng lưu trạng thái của các kết nối mạng. Dựa trên vị trí các lớp giao thức mạng, có thể chia tường lửa thành 3 loại: tường lửa lọc gói (Packet-filtering), cổng ứng dụng (Application-level gateway) và cổng chuyển mạch (Circuit-level gateway). Tường lửa lọc gói thường thực hiện việc lọc các gói tin IP, theo đó một tập, hoặc một nhóm các luật được áp dụng cho mỗi gói tin gửi đi, hoặc chuyển đến để quyết định chuyển tiếp các gói tin hợp pháp, hay loại bỏ gói tin bất hợp pháp. Cổng ứng dụng, còn gọi là máy chủ proxy thường được sử dụng để phát lại lưu lượng mạng ở mức ứng dụng. Cổng ứng dụng thực hiện việc lọc các yêu cầu, hoặc hồi đáp (request/response) ở các giao thức ứng dụng phổ biến như HTTP, SMTP, FTP,... Cổng chuyển mạch hoạt động ở mức thấp nhất, với cơ chế tương tự như các bộ chuyển mạch (switch). Hình 4.16 minh họa mô hình tường lửa lọc gói (a), cổng ứng dụng (b) và cổng chuyển mạch (c).



Hình 4.15. Hệ thống tường lửa bảo vệ các máy chủ dịch vụ và máy trạm

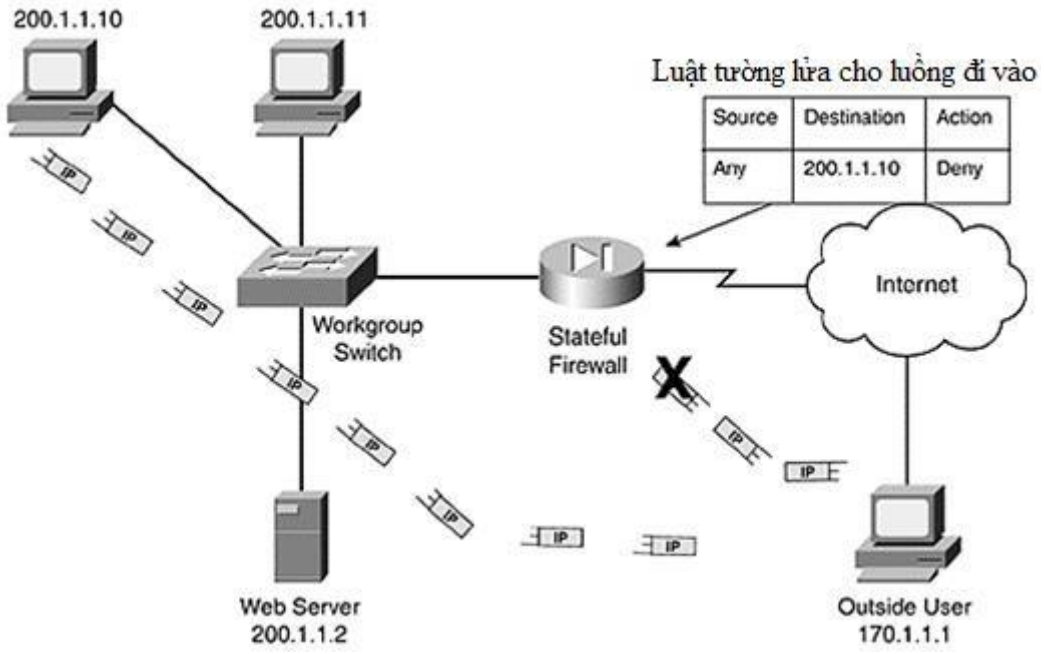


Hình 4.16. Mô hình tường lửa lọc gói (a), Cổng ứng dụng (b) và Cổng chuyển mạch (c)

Dựa trên khả năng lưu trạng thái của các kết nối mạng, tường lửa được chia thành 2 loại: tường lửa có trạng thái (Stateful firewall) và tường lửa không trạng thái (Stateless firewall). Tường lửa có trạng thái có khả năng lưu trạng thái của các kết nối mạng đi qua và được lập trình để phân biệt các gói tin thuộc về các kết nối mạng khác nhau. Theo đó, chỉ những gói tin thuộc một kết nối mạng đang hoạt động mới được đi qua tường lửa, còn các gói tin khác không thuộc kết nối đang hoạt động sẽ bị chặn lại. Hình 4.17 minh hoạt một tường lửa có

trạng thái chặn các gói tin IP gửi từ người dùng ngoài (Outside User) đến địa chỉ IP 200.1.1.10 do chúng không thuộc kết nối đang hoạt động. Ngược lại, tường lửa không trạng thái thực hiện việc lọc các gói tin riêng rẽ mà không quan tâm mỗi gói tin thuộc về kết nối mạng nào. Tường lửa dạng này dễ bị tấn công bởi kỹ thuật giả mạo

địa chỉ, giả mạo nội dung gói tin do tường lửa không có khả năng nhớ các gói tin đi trước thuộc cùng một kết nối mạng.



Hình 4.17. Tường lửa có trạng thái chặn gói tin không thuộc kết nối đang hoạt động

1.3 Các kỹ thuật kiểm soát truy nhập

Hầu hết các tường lửa hỗ trợ nhiều kỹ thuật kiểm soát truy nhập, gồm kiểm soát dịch vụ, kiểm soát hướng, kiểm soát người dùng và kiểm soát hành vi. Cụ thể:

- Kiểm soát dịch vụ xác định dịch vụ nào có thể được truy nhập và thường được thực hiện thông qua việc mở hoặc đóng một cổng dịch vụ nào đó. Chẳng hạn, để cung cấp dịch vụ web và cấm tất cả các dịch vụ khác, tường lửa mở cổng HTTP 80 và HTTPS 443, còn đóng tất cả các cổng dịch vụ khác.
- Kiểm soát hướng điều khiển hướng được phép đi của các gói tin của mỗi dịch vụ. Hướng có thể gồm luồng từ mạng nội bộ đi ra (outgoing) và luồng từ ngoài đi vào mạng nội bộ (incoming).
- Kiểm soát người dùng xác định người dùng nào được quyền truy nhập và thường áp dụng cho người dùng mạng nội bộ.

- Kiểm soát hành vi thực hiện kiểm soát việc sử dụng các dịch vụ cụ thể. Ví dụ như, tường lửa có thể được cấu hình để lọc loại bỏ các thư rác, hoặc hạn chế truy nhập đến một bộ phận thông tin của máy chủ web.

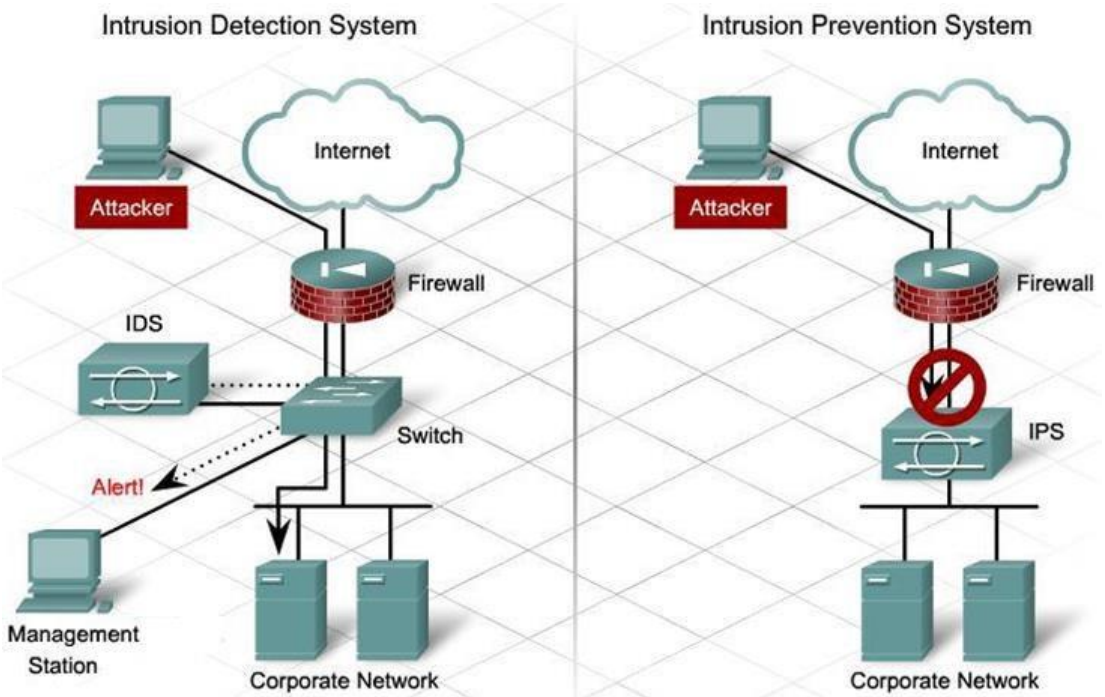
1.4 Các hạn chế của tường lửa

Mặc dù tường lửa được sử dụng rộng rãi để bảo vệ mạng nội bộ khỏi các cuộc tấn công, xâm nhập, nhưng cũng như hầu hết các kỹ thuật và công cụ đảm bảo an toàn khác, tường lửa cũng có những hạn chế. Các hạn chế của tường lửa gồm:

- Không thể chống lại các tấn công không đi qua tường lửa. Đó có thể là các dạng tấn công khai thác yếu tố con người, hoặc kẻ tấn công có thể xâm nhập trực tiếp vào hệ thống mạng nội bộ mà không đi qua tường lửa.
- Không thể chống lại các tấn công hướng dữ liệu, hoặc tấn công vào các lỗ hổng bảo mật của các phần mềm.
- Không thể chống lại các hiểm hoạ từ bên trong, như từ người dùng trong mạng nội bộ.
- Không thể ngăn chặn việc vận chuyển các chương trình hoặc các file bị nhiễm vi rút hoặc các phần mềm độc hại (thường ở dạng nén hoặc mã hóa).

2. Các hệ thống phát hiện và ngăn chặn xâm nhập

2.1 Giới thiệu



Hình 4.18. Vị trí các hệ thống IDS và IPS trong sơ đồ mạng

Các hệ thống phát hiện, ngăn chặn tấn công, xâm nhập (IDS/IPS) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng theo mô hình phòng thủ có chiều sâu (defence in depth). IDS (Intrusion Detection System) là hệ thống phát hiện tấn công, xâm nhập và IPS (Intrusion Prevention System) là hệ thống ngăn chặn tấn công, xâm nhập. Các hệ thống IDS/IPS có thể được đặt trước hoặc sau tường lửa trong mô hình mạng, tùy theo mục đích sử dụng. Hình 4.18 cung cấp vị trí các hệ thống IDS và IPS trong sơ đồ mạng, trong đó IDS thường được kết nối vào bộ switch phía sau tường lửa, còn IPS được ghép vào giữa đường truyền từ cổng mạng, phía sau tường lửa.

Nhiệm vụ chính của các hệ thống IDS/IPS bao gồm:

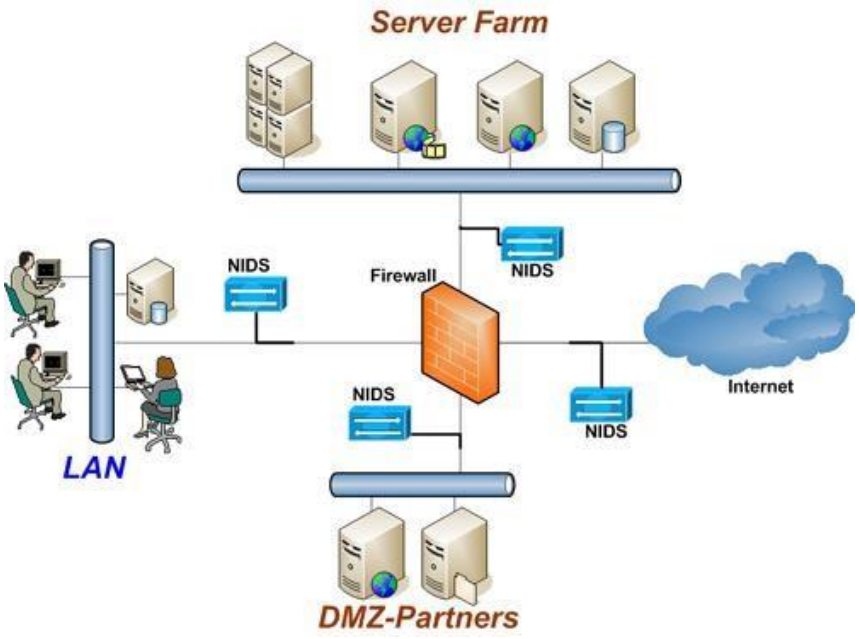
- Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập;
- Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi logs các hành vi này cho phân tích bổ sung sau này;
- Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập;
- Gửi thông báo cho người quản trị về các các hành vi tấn công, xâm nhập đã phát hiện được.

Về cơ bản IPS và IDS giống nhau về chức năng giám sát lưu lượng mạng hoặc các sự kiện trong hệ thống. Tuy nhiên, IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công, xâm nhập bị phát hiện. Trong khi đó, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

2.2 Phân loại

Có 2 phương pháp phân loại chính các hệ thống IDS và IPS, gồm (1) phân loại theo nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu. Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS):
  NIDS phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng.
  Hình 4.19 biểu diễn một sơ đồ mạng, trong đó các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng.

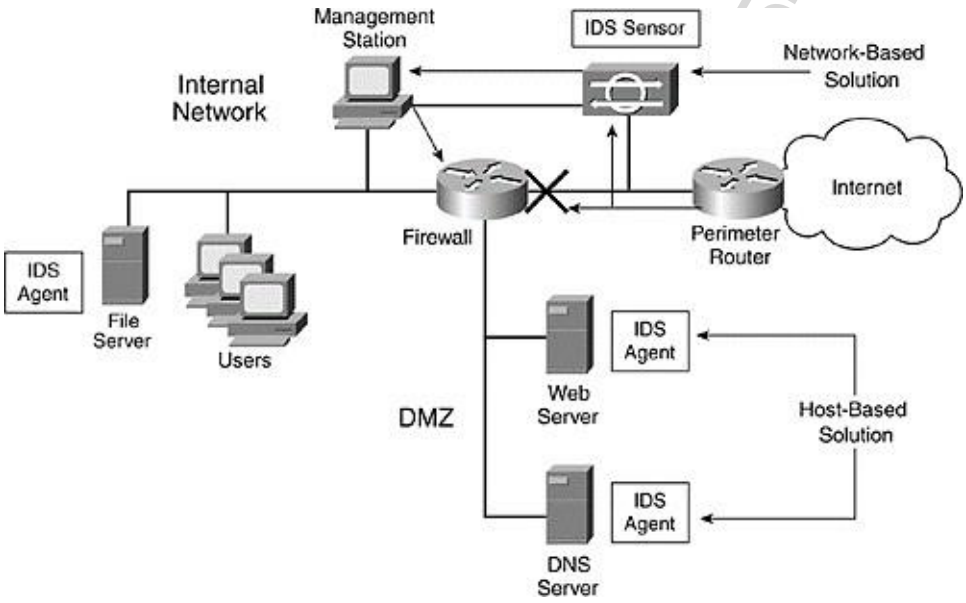


Hình 4.19. Các NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng

- Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS): HIDS phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó. Hình 4.20 minh họa một sơ đồ mạng, trong đó sử dụng NIDS để giám sát lưu lượng tại cổng mạng và HIDS để giám sát các host thông qua các IDS agent. Một trạm quản lý (Management station) được thiết lập để thu nhập các thông tin từ các NIDS và HIDS để xử lý và đưa ra quyết định cuối cùng.

Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phân tích chính, gồm (1) phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng (Signature-based / misuse

intrusion detection) và (2) phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection). Mục tiếp theo trình bày chi tiết hơn về hai kỹ thuật phát hiện này.

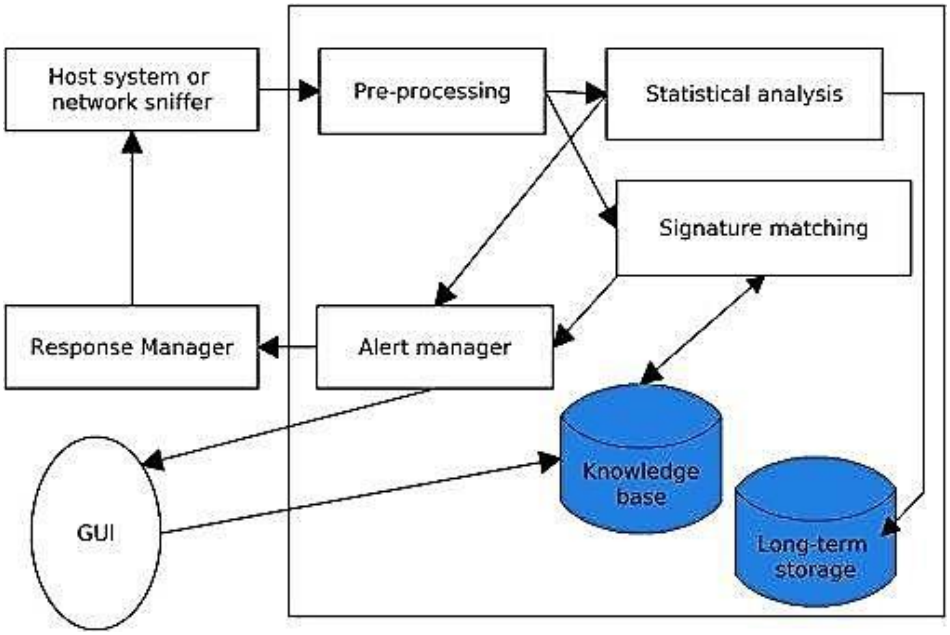


Hình 4.20. Sử dụng kết hợp NIDS và HIDS để giám sát lưu lượng mạng và các host

2.3 Các kỹ thuật phát hiện xâm nhập

2.3.1 Phát hiện xâm nhập dựa trên chữ ký

Phát hiện xâm nhập dựa trên chữ ký trước hết cần xây dựng cơ sở dữ liệu các chữ ký, hoặc các dấu hiệu của các loại tấn công, xâm nhập đã biết. Hầu hết các chữ ký, dấu hiệu được nhận dạng và mã hóa thủ công và dạng biểu diễn thường gặp là các luật phát hiện (Detection rule). Bước tiếp theo là sử dụng cơ sở dữ liệu các chữ ký để giám sát các hành vi của hệ thống, hoặc mạng, và cảnh báo nếu phát hiện chữ ký của tấn công, xâm nhập. Hình 4.21 biểu diễn lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký điển hình.

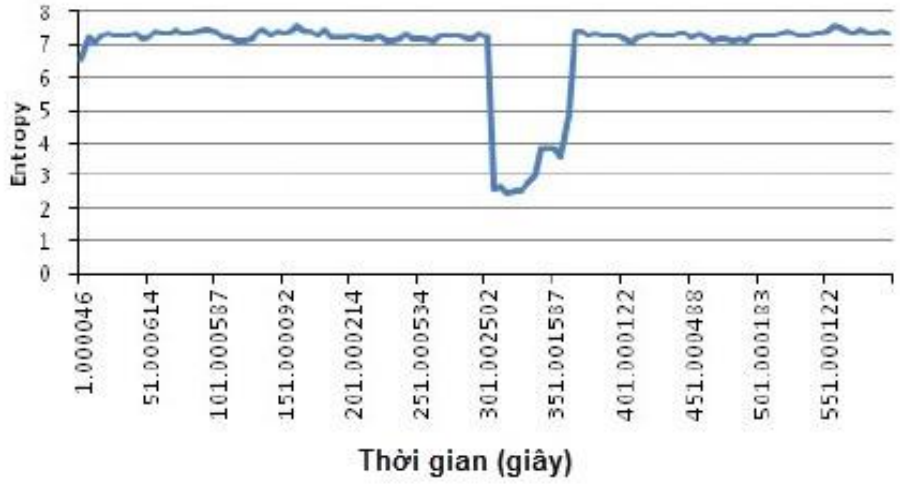


Hình 4.21. Lưu đồ giám sát phát hiện tấn công, xâm nhập dựa trên chữ ký

Ưu điểm lớn nhất của phát hiện xâm nhập dựa trên chữ ký là có khả năng phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả. Ngoài ra, phương pháp này cho tốc độ xử lý cao, đồng thời yêu cầu tài nguyên tính toán tương đối thấp. Nhờ vậy, các hệ thống phát hiện xâm nhập dựa trên chữ ký được ứng dụng rộng rãi trong thực tế. Tuy nhiên, nhược điểm chính của phương pháp này là không có khả năng phát hiện các tấn công, xâm nhập mới, do chữ ký của chúng chưa tồn tại trong cơ sở dữ liệu các chữ ký. Hơn nữa, nó cũng đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công, xâm nhập.

2.3.2 Phát hiện xâm nhập dựa trên bất thường

Phát hiện xâm nhập dựa trên bất thường dựa trên giả thiết: *các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường*. Quá trình xây dựng và triển khai một hệ thống phát hiện xâm nhập dựa trên bất thường gồm 2 giai đoạn: (1) huấn luyện và (2) phát hiện. Trong giai đoạn huấn luyện, hồ sơ (profile) của đối tượng trong chế độ làm việc bình thường được xây dựng. Để thực hiện giai đoạn huấn luyện này, cần giám sát đối tượng trong một khoảng thời gian đủ dài để thu thập được đầy đủ dữ liệu mô tả các hành vi của đối tượng trong điều kiện bình thường làm dữ liệu huấn luyện. Tiếp theo, thực hiện huấn luyện dữ liệu để xây dựng mô hình phát hiện, hay hồ sơ của đối tượng. Trong giai đoạn phát hiện, thực hiện giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và các hành vi lưu trong hồ sơ của đối tượng.



Hình 4.22. Giá trị entropy của IP nguồn của các gói tin từ lưu lượng hợp pháp (phần giá trị cao, đều) và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS (phần giá trị thấp)

Hình 4.22 biểu diễn giá trị entropy của IP nguồn của các gói tin theo cửa sổ trượt từ lưu lượng bình thường và entropy của IP nguồn của các gói tin từ lưu lượng tấn công DDoS. Có thể thấy sự khác biệt rõ nét giữa giá trị entropy của lưu lượng bình thường và lưu lượng tấn công và như vậy, nếu một ngưỡng entropy được chọn phù hợp ta hoàn toàn có thể phát hiện sự xuất hiện của cuộc tấn công DDoS dựa trên sự thay đổi đột biến của giá trị entropy.

Ưu điểm của phát hiện xâm nhập dựa trên bất thường là có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin về chúng. Tuy nhiên, phương pháp này có tỷ lệ cảnh báo sai tương đối cao so với phương pháp phát hiện dựa trên chữ ký. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bất thường. Ngoài ra, nó cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại.