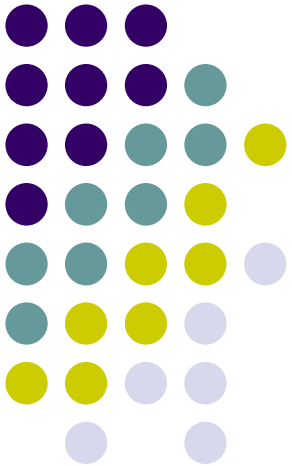
Chương 3

Hạ tầng cơ sở và kết nối



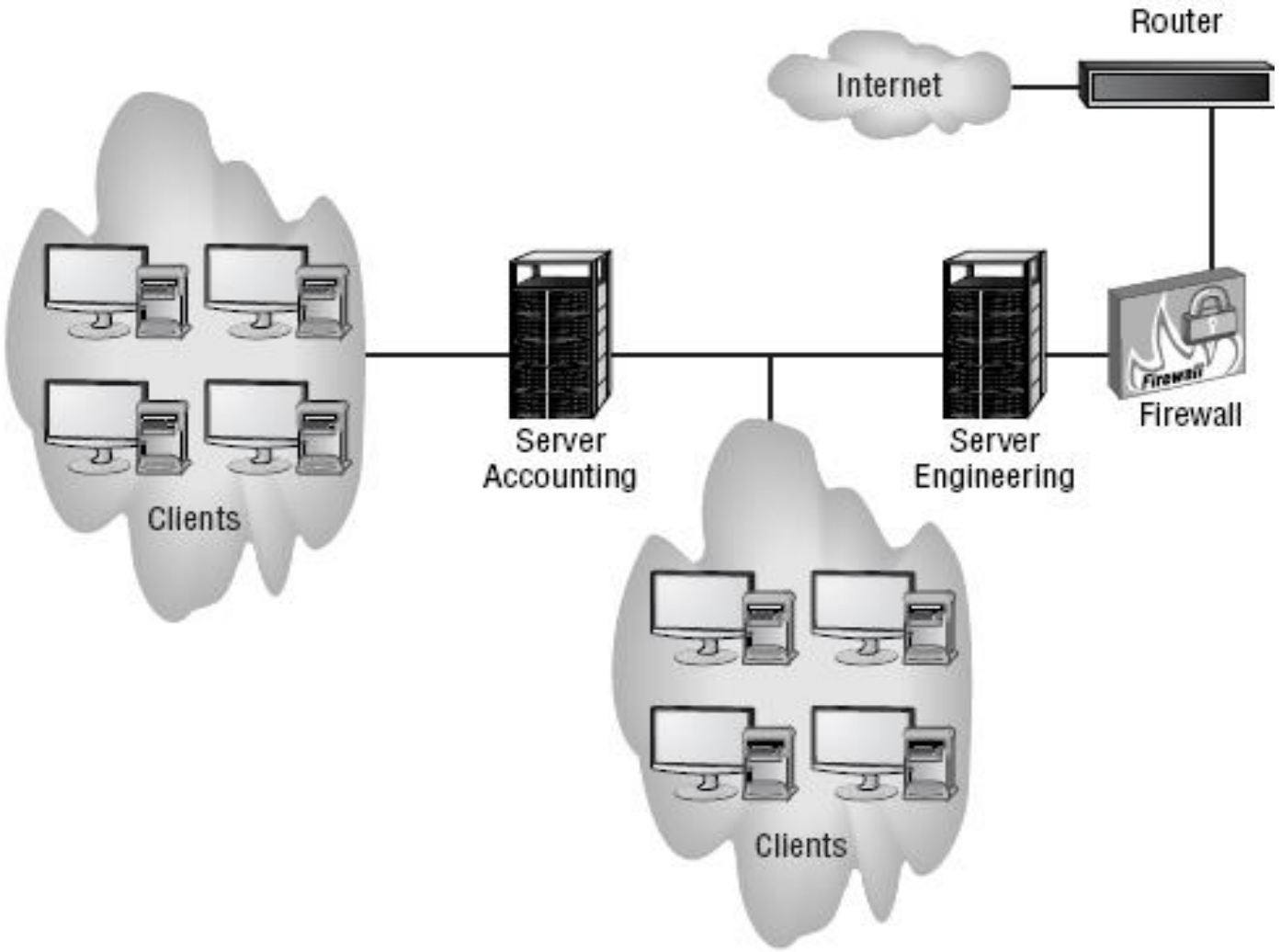
Nội dung

- Bảo mật cơ sở hạ tầng
- Sự khác biệt của các thiết bị mạng nền tảng
- Kiểm tra và phân tích mạng
- Bảo mật máy trạm và máy chủ
- Các thiết bị di động
- Truy cập từ xa
- Bảo mật các kết nối Internet
- Giao thức SNMP và các giao thức TCP/IP khác
- Đặc điểm cơ bản của cáp, dây nối và giao tiếp
- Khai thác phương tiện lưu trữ

3.1 Bảo mật cơ sở hạ tầng

- Liên quan đến khía cạnh cơ bản nhất của dòng thông tin và cách làm việc trong hệ thống mạng.
- Cơ sở hạ tầng là nền tảng cho tất cả các công việc trong tổ chức
- Thành phần phần cứng - Các thiết bị trong hạ tầng:
  - Router
  - Firewall
  - Switch
  - Server
  - Workstation

Cơ sở hạ tầng


Router
Internet
Clients
Server
Accounting
Server
Engineering
Firewall
Clients

Cơ sở hạ tầng

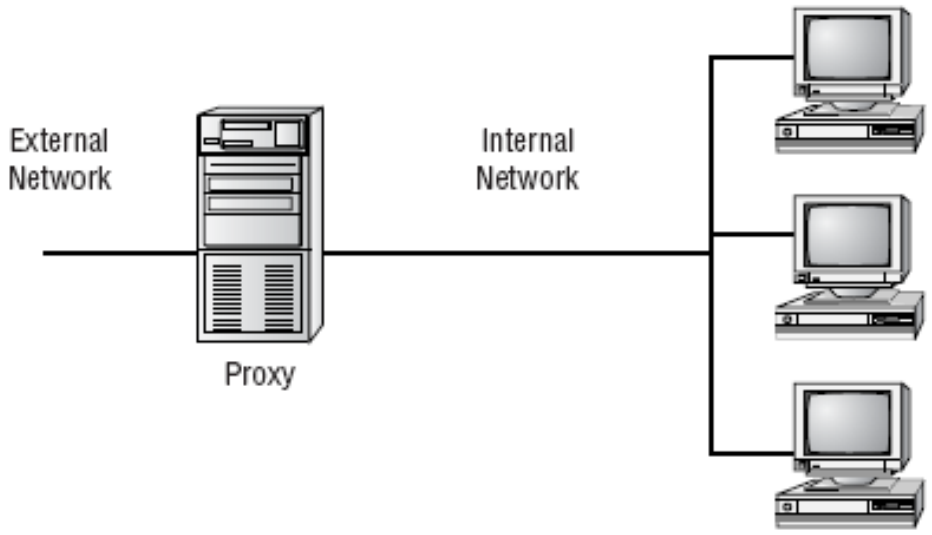
- Thành phần phần mềm
  - Nhiều hệ thống làm việc độc lập
  - Cần có một trung tâm điều hành quản lý chung NOC (Network Operator Center)

3.2 Các thiết bị nền tảng

- **Phần cứng bảo mật mạng**
- Các thiết bị phần cứng được thiết kế đặc biệt
  - Bảo mật tốt hơn so với các thiết bị mạng thông thường
- Các dạng phần cứng bảo mật mạng
  - Tường lửa (Firewall)
  - Ủy nhiệm (Proxy)
  - Bộ lọc thư rác (Spam Filter)
  - Bộ lọc nội dung Internet (Internet Content Filter)
  - Cổng bảo mật Web (Web Security Gateway)
  - Phát hiện và ngăn chặn việc thâm nhập
  - Thiết bị bảo mật mạng tất cả trong một bảo mật mạng

Firewall

- Firewall
  - Packet filter
  - Proxy firewall
  - Stateful inspection



Firewall

- Tường lửa (firewall) là một thiết bị chuyên dụng, hoặc một máy tính được cài đặt phần mềm chuyên dụng dùng để lọc hoặc hạn chế lưu lượng giữa các mạng một cách có lựa chọn.
- Chức năng chính là điều khiển kiểm soát truy cập:
  - Kiểm soát dịch vụ
  - Kiểm soát hướng
  - Kiểm soát người dùng
  - Kiểm soát hành vi

Firewall

- Tường lửa thường kết hợp cả phần cứng và phần mềm, và nằm giữa hai mạng riêng nối với nhau hoặc thường nằm giữa một mạng riêng và mạng Internet -> **tường lửa mạng (network-based firewall)**
- Một loại tường lửa khác được gọi là **tường lửa theo máy (host-based firewall)** chỉ bảo vệ máy tính mà chúng được cài đặt.
- Hiện nay có nhiều loại tường lửa, chúng có thể được cài đặt bằng nhiều cách khác nhau.

Hình 4-3 Vị trí tường lửa giữa mạng riêng và Internet

Packet-filtering firewall

- Dạng đơn giản nhất của tường lửa là **tường lửa lọc gói tin (packet-filtering firewall)**
  - Là một router (hoặc một máy tính cài đặt phần mềm cho phép nó hoạt động như một router) kiểm tra header của tất cả các gói tin của dữ liệu mà nó nhận được
  - Để xác định liệu gói tin dạng này có được phép tiếp tục gửi đến đích của nó.
- Nếu một gói tin không đáp ứng các tiêu chí lọc, tường lửa sẽ chặn các gói tin này lại.
- Nếu một gói tin đáp ứng các tiêu chí lọc, tường lửa sẽ cho phép gói tin đi qua mạng kết nối với tường lửa.
- Thực tế, gần như tất cả các router có thể được cấu hình để hoạt động như một tường lửa lọc gói tin.

Packet-fitering firewall

- Ngoài việc chặn lưu lượng *vào* một mạng LAN, tường lửa lọc gói tin có thể chặn lưu lượng *đi ra* khỏi một mạng LAN.
- Một lý do để chặn lưu lượng gửi đi là để ngăn chặn sâu máy tính lây lan.
- Ví dụ, trên một Web server: trong hầu hết các trường hợp server này chỉ trả lời các yêu cầu gửi đến và không cần phải khởi tạo các yêu cầu gửi đi
  - Có thể cấu hình tường lửa lọc gói tin để chặn các gói tin gửi ra ngoài được khởi tạo từ Web server.
  - Bằng cách này sẽ giúp chặn các sâu máy tính lây lan được lập trình nhằm gắn vào Web server và tự lan truyền đến các máy tính khác trên Internet

Packet-fitering firewall

- Một số tiêu chí chung của tường lửa lọc gói tin có thể dùng để cho phép hoặc từ chối lưu lượng bao gồm:
  - Địa chỉ IP nguồn và đích
  - Các cổng nguồn và đích (ví dụ các cổng hỗ trợ kết nối TCP/UDP, FTP, Telnet, ARP, ICMP, …)
  - Các cờ thiết lập trong IP header (ví dụ SYN hay ACK)
  - Quá trình truyền dữ liệu sử dụng giao thức UDP hay ICMP
  - Trạng thái của gói tin là gói tin đầu tiên của một luồng dữ liệu mới hay một gói tin tiếp theo
  - Trạng thái của gói tin là gói tin gửi đến hay gửi đi từ mạng riêng của bạn

Firewall

Để bảo mật tốt hơn, nên chọn một tường lửa có thể thực hiện các chức năng phức tạp hơn :

- Tường lửa có hỗ trợ mã hóa
- Tường lửa có hỗ trợ xác thực người dùng
- Tường lửa lọc nội dung **(content-filtering firewall)** có thể chặn các lưu lượng dựa trên dữ liệu ứng dụng được chứa trong gói tin
- Tường lửa có cho phép chức năng ghi nhật ký và kiểm tra như IDS / IPS
- Tường lửa có thể theo dõi một luồng dữ liệu từ đầu đến cuối **tường lửa có trạng thái (stateful firewall)**
- Tường lửa phi trạng thái làm việc nhanh hơn so với tường lửa có trạng thái

Vai trò Firewall

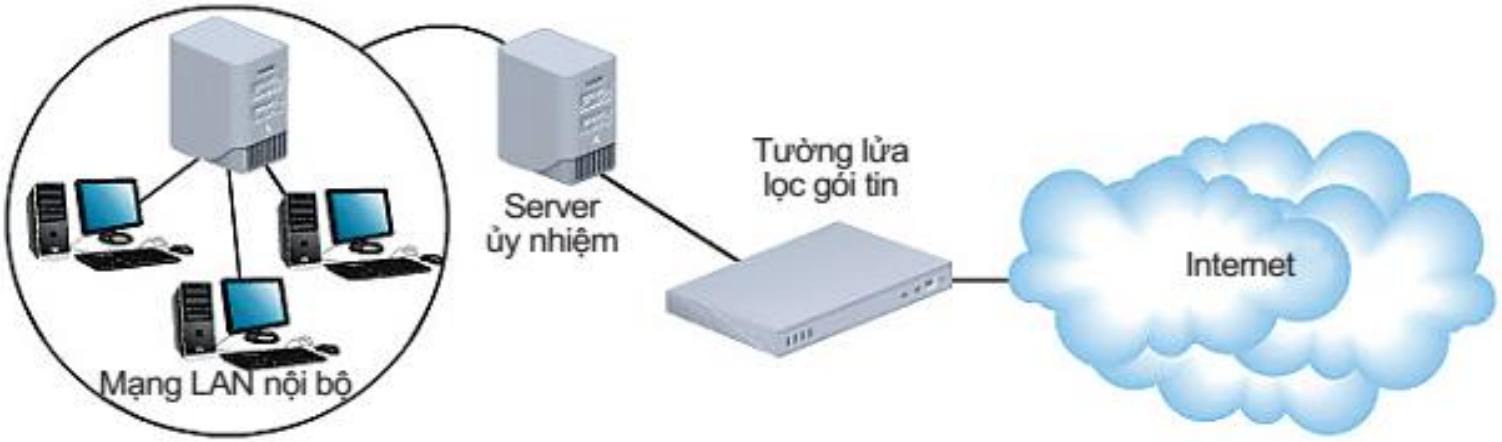
- Làm được
  - Kiểm soát luồng dữ liệu đi qua nó
  - Bảo vệ các lớp bên trong
  - Cấm tất cả. Cấu hình những gì cho qua
  - Cho phép tất cả, cấu hình những gì cấm
  - Ghi nhận & báo cáo sự kiện
- Không làm được
  - Viruses
  - Lỗi con người (vô tình, cố ý)
  - Kết nối hở
  - Chính sách tồi
  - Social Engineering

Firewall

- Phải xây dựng tường lửa theo nhu cầu của mạng
  - Không chỉ đơn giản là mua, cài đặt nó giữa mạng LAN và Internet
  - trông chờ nó sẽ cung cấp bảo mật nhiều hơn.
- Trước tiên phải xem xét những loại lưu lượng muốn lọc, sau đó cấu hình tường lửa cho phù hợp.
  - Để đạt được cấu hình tốt nhất có thể phải mất tới vài tuần
- Không nên thiết lập quá nghiêm ngặt dẫn đến việc chặn người dùng có thẩm quyền gửi và nhận dữ liệu cần thiết,
- Cũng không nên quá nới lỏng sẽ gây nên nguy cơ vi phạm an ninh mạng.

Proxy - Server ủy nhiệm

- Một PP tăng cường an ninh tầng Mạng và tầng Giao vận dùng tường lửa là kết hợp tường lửa lọc gói tin và dịch vụ ủy nhiệm.
- **Dịch vụ ủy nhiệm (proxy service)** là một phần mềm ứng dụng chạy trên một host, đóng vai trò trung gian giữa mạng bên ngoài và nội bộ, thẩm định tất cả lưu lượng vào và ra.
- Các host mạng chạy dịch vụ ủy nhiệm được gọi là **server ủy nhiệm**.
  - **application gateway / proxy**.
  - Server ủy nhiệm quản lý an ninh ở tầng Ứng dụng của mô hình OSI.



Proxy - Server ủy nhiệm

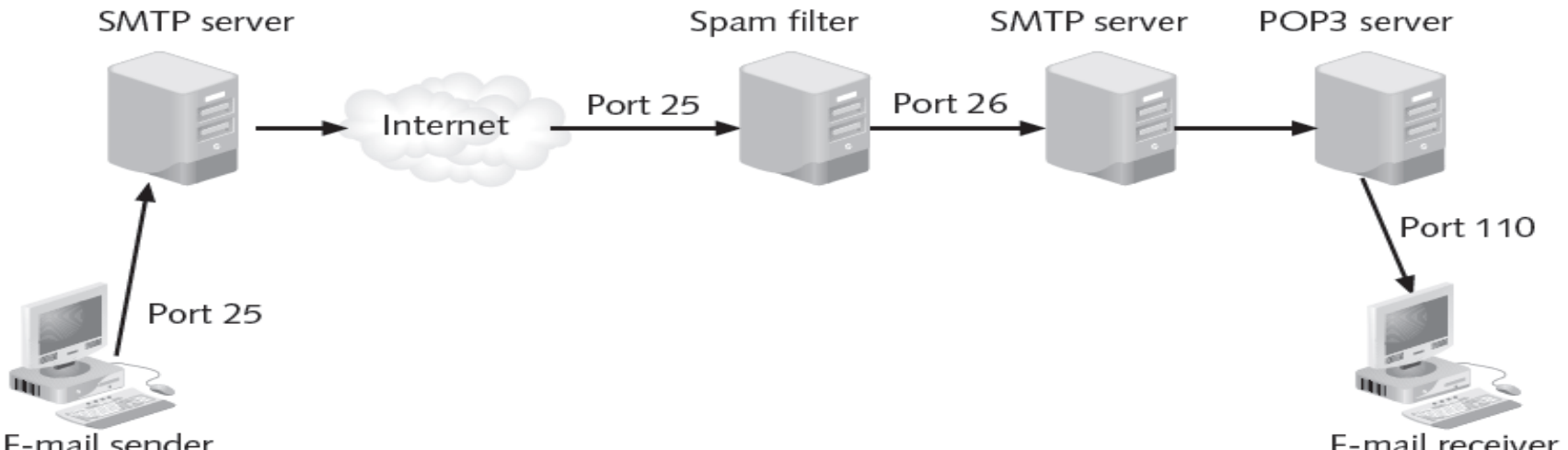
- Server ủy nhiệm cũng có thể cải thiện hiệu năng cho người dùng khi truy cập vào các tài nguyên bên ngoài mạng của họ bằng cách lưu đệm các fie.
- Ví dụ, 1 server ủy nhiệm (nằm giữa mạng LAN và một Web server bên ngoài) có thể được cấu hình để lưu lại các trang web được xem gần đây.
  - Sau đó người dùng trong LAN muốn xem một trong những trang web đã lưu, server ủy nhiệm sẽ gửi nội dung về.
- Điều này giúp ta giảm bớt khoảng thời gian đi qua mạng WAN và lấy nội dung từ Web server bên ngoài.

Bộ lọc thư rác – phần cứng

- Bộ lọc thư rác (spam filter)
  - Các bộ lọc thư rác cấp doanh nghiệp có thể chặn các thư rác trước khi chúng đi tới máy chủ
- Các hệ thống email sử dụng hai giao thức
  - Simple Mail Transfer Protocol (SMTP)
    - Xử lý mail gửi đi
  - Post Office Protocol (POP)
    - Xử lý mail gửi đến

Bộ lọc thư rác – phần cứng

- Các bộ lọc thư rác được cài đặt với máy chủ SMTP
  - Bộ lọc được cấu hình để "nghe" tại cổng 25
  - Những thư điện tử không phải thư rác được chuyển tới máy chủ SMTP đang "nghe" tại một cổng khác
- Phương pháp ngăn không cho máy chủ SMTP gửi lại thông báo cho kẻ gửi thư rác biết việc phân phát thư rác bị thất bại



Bộ lọc nội dung Internet – phần cứng

- Bộ lọc nội dung Internet
  - Kiểm soát lưu lượng mạng Internet
  - Chặn truy cập tới các web site và file được lựa chọn trước
  - Các web site bị chặn được xác định thông qua URL hoặc thông qua đối chiếu từ khóa

Cổng bảo mật Web

- Cổng bảo mật Web (Web security gateway)
  - Có thể chặn các nội dung độc hại trong thời gian thực Chặn nội dung thông qua việc lọc ở cấp ứng dụng
- Ví dụ về lưu lượng Web bị chặn
  - Các đối tượng ActiveX
  - Phần mềm quảng cáo, phần mềm gián điệp Việc chia sẻ dữ liệu ngang hàng (peer-to-peer) Khai thác mã kịch bản

Phát hiện và ngăn chặn thâm nhập

- Bảo mật thụ động và bảo mật chủ động có thể được áp dụng trong mạng
  - Các biện pháp chủ động đem lại mức an toàn cao hơn
- Biện pháp thụ động
  - Tường lửa
  - Bộ lọc nội dung Internet
- Hệ thống phát hiện thâm nhập (IDS)
  - Biện pháp bảo mật chủ động
  - Có thể phát hiện tấn công ngay khi nó xảy ra
- Các khía cạnh của IDS
  - Các phương pháp giám sát Các dạng IDS

Các phương pháp giám sát

Các phương pháp giám sát (monitoring methodology)

- Giám sát dựa trên sự bất thường (anomaly-based monitoring)
  - So sánh hành vi phát hiện được với đường cơ sở
- Giám sát dựa trên chữ ký (signature-based monitoring)
  - Tìm kiếm các đặc điểm, dấu hiệu đặc trưng của tấn công
- Giám sát dựa trên hành vi (behavior-based monitoring)
  - Phát hiện các hành vi bất thường của tiến trình hay chương trình
  - Cảnh báo người dùng để họ đưa ra quyết định chặn hay cho phép hành vi
- Giám sát kiểu tự khám phá (heuristic monitoring)
  - Sử dụng các kỹ thuật dựa trên kinh nghiệm

Hệ thống phát hiện thâm nhập IDS

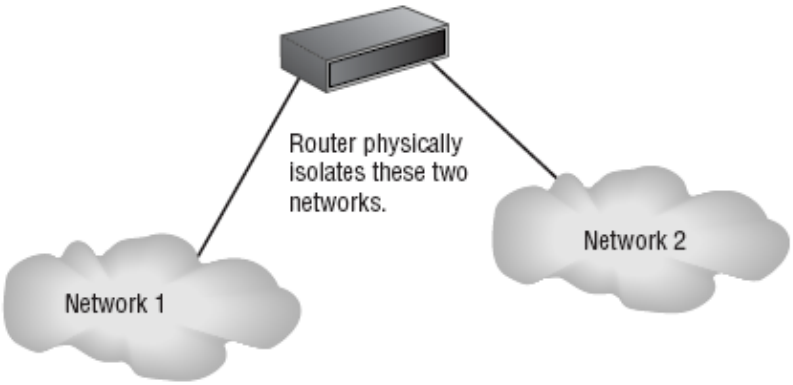
- **Các dạng IDS :**
  - Hệ thống phát hiện xâm nhập máy chủ (Host Intrusion Detection System - HIDS)
  - Hệ thống phát hiện xâm nhập mạng (Network Intrusion Detection System - NIDS)
  - Hệ thống ngăn chặn xâm nhập mạng (Network Intrusion Prevention - NIPS)

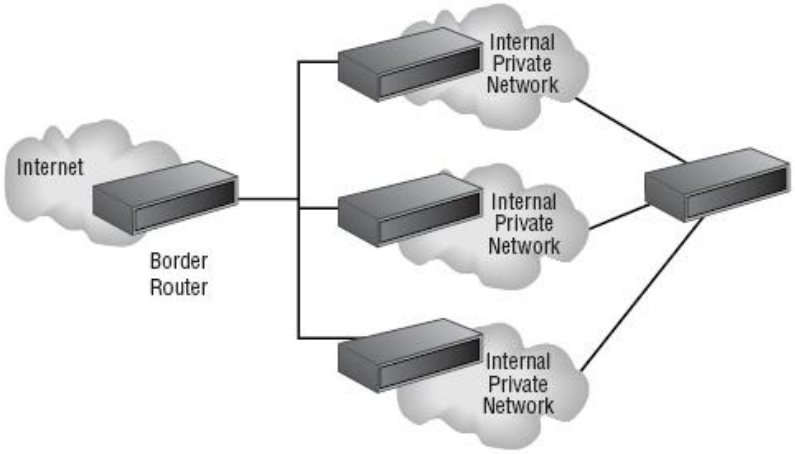
Thiết bị bảo mật mạng tất cả trong một

- Các thiết bị bảo mật mạng tất cả trong một
  - Một thiết bị tích hợp thay thế cho nhiều thiết bị bảo mật
- Xu hướng gần đây:
  - Kết hợp các thiết bị bảo mật đa năng với thiết bị truyền thống như bộ định tuyến
- **Ưu điểm của phương pháp**
  - Khi thiết bị mạng xử lý xong các gói tin
  - Bộ chuyển mạch (switch) chứa phần mềm anti-malware kiểm tra các gói tin và chặn lại trước khi chuyển đi để không bị lây nhiễm toàn mạng

Các thiết bị nền tảng

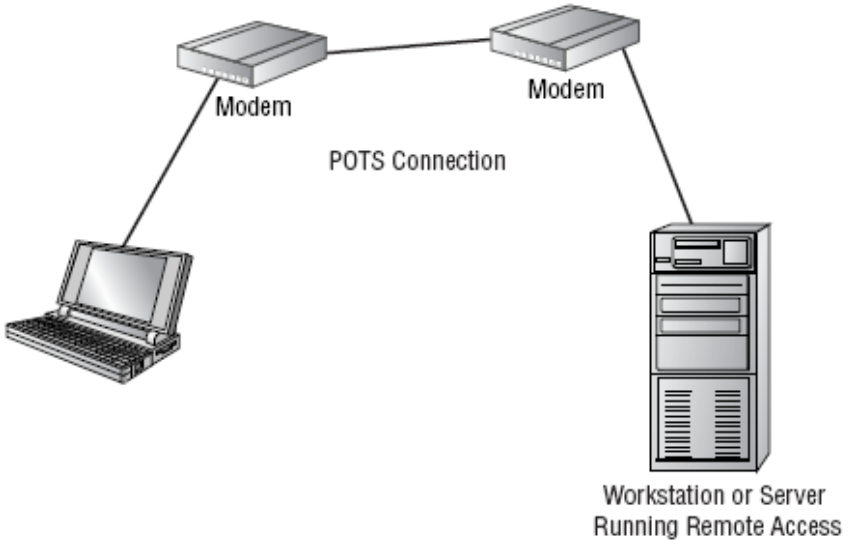
- Hub
- Router





Các thiết bị nền tảng

- Switch
- Wireless AP
- Modem
- RAS
- Telecom/PBX
- VPN



3.3 Kiểm tra và phân tích mạng

- Quá trình sử dụng thiết bị nắm bắt dữ liệu hoặc sử dụng pp khác để chặn thông tin từ mạng
- 2 loại:
  - Sniffer
  - Hệ thống phát hiện xâm nhập (IDS)
- Sniffer:
  - PC, NIC card, phần mềm kiểm tra
- **IDS (Intrusion detection system - hệ thống phát hiện xâm nhập)**
  - Phần mềm chạy trên workstation hoặc thiết bị mạng kiểm tra và theo dõi các hoạt động mạng
  - Có khả năng nhận biết những hoạt động khả nghi / hành động xâm nhập trái phép trên mạng trong tiến trình tấn công (FootPrinting, Scanning, Sniffer…)
  - Có thể cấu hình alarm, phân tích đánh giá log,…
  - Được bán kèm với firewall.

IDS

- IDS là một phần mềm chạy trên một máy tính (server) hoặc trên các thiết bị kết nối (switch).
- Một chương trình IDS chạy trên một máy tính mà cho phép truy cập từ Internet được gọi là **HIDS (**host-based intrusion detection – Phát hiện xâm nhập theo host**).**
- Phát hiện xâm nhập xảy ra trên các thiết bị nằm ở biên của mạng, hay nơi xử lý toàn bộ các lưu lượng được gọi là **NIDS (**network-based intrusion detection **–** Phát hiện xâm nhập theo mạng**).**
- Việc sử dụng biện pháp an ninh toàn diện kết hợp cả HIDS và NIDS sẽ giúp phát hiện nhiều mối đe dọa ở phạm vi rộng hơn và thiết lập nhiều lớp phòng bị.
- Ví dụ, HIDS có thể phát hiện việc cố gắng khai thác một ứng dụng không an toàn nào đó mà NIDS bỏ qua.

IDS

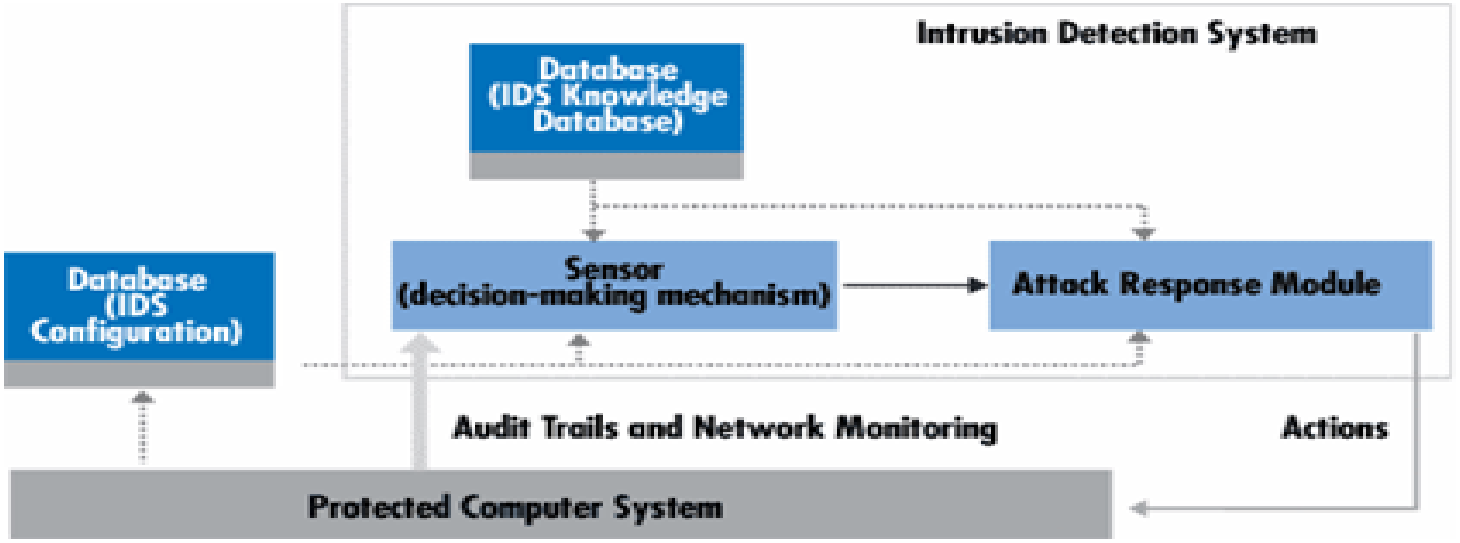
- Các nhà cung cấp phần cứng mạng lớn như Cisco, HP, Juniper Networks, và Lucent đều bán thiết bị IDS.
- Ví dụ về các phần mềm IDS mã nguồn mở phổ biến hầu như có thể chạy trên bất kỳ máy tính nối mạng nào là
  - **Tripwire**
  - **Snort**
- Một kỹ thuật mà IDS có thể sử dụng để theo dõi lưu lượng đi qua một switch là **phản chiếu cổng (port mirroring)**.
- Trong **phản chiếu cổng**, một cổng được cấu hình để gửi đi một bản sao của tất cả các lưu lượng đi qua cổng đó đến một cổng thứ hai trên switch.
  - Cổng thứ hai gửi lưu lượng sao chép đó đến một chương trình giám sát.

IDS

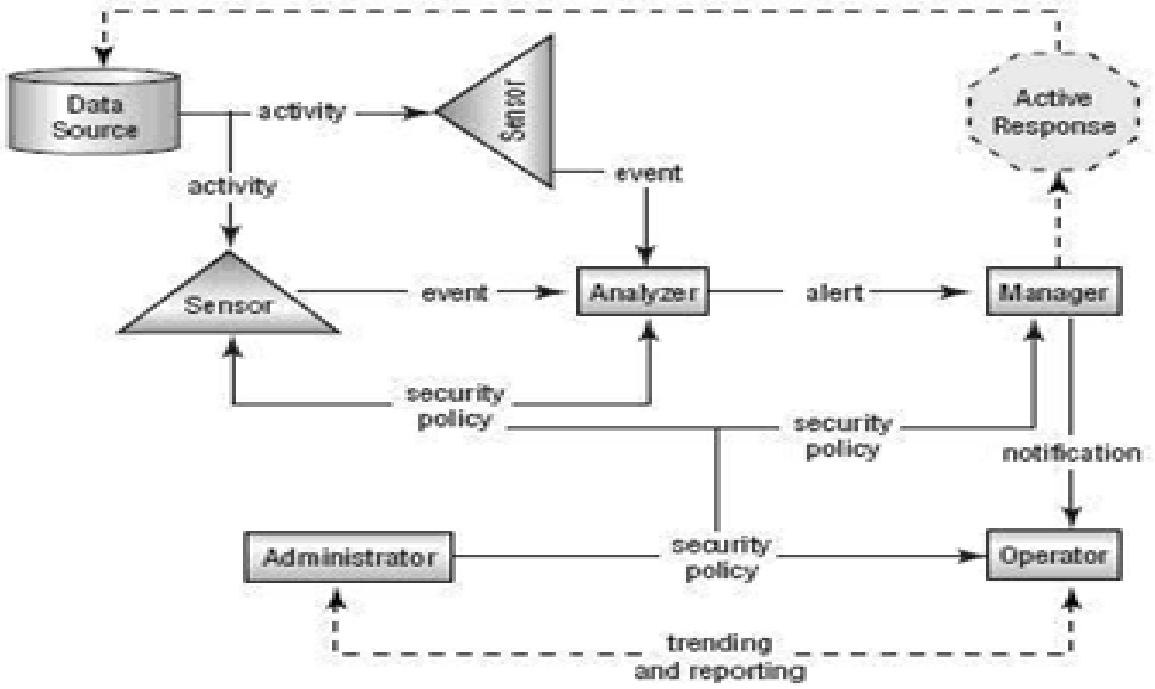
- Một nhược điểm khi sử dụng IDS tại DMZ của mạng là số lượng các xác nhận sai mà nó có thể ghi lại.
  - Ví dụ, nó có thể hiểu sự đăng nhập nhiều lần của người sử dụng hợp pháp (ví dụ khi anh ta quên mật khẩu) là một sự đe dọa an toàn và bảo mật.
- Nếu IDS được cấu hình để cảnh báo cho quản trị mạng (SMS) -> có thể bị quá tải với những cảnh báo như vậy và cuối cùng bỏ qua tất cả SMS của IDS.
  - Vì vậy, phần mềm IDS cần phải được tùy chỉnh cẩn thận.
- Ngoài ra, để tiếp tục bảo vệ chống lại các mối đe dọa mới, phần mềm IDS phải được cập nhật và các quy tắc phát hiện phải được đánh giá lại một cách thường xuyên.

IDS

- Một IDS cần phải thỏa mãn những yêu cầu sau:
  - Tính chính xác : không được coi những hành động thông thường trong môi trường hệ thống là những hành động bất thường hay lạm dụng (false positive).
  - Hiệu năng : phải đủ để phát hiện xâm nhập trái phép trong thời gian thực (nghĩa là hành động xâm nhập trái phép phải được phát hiện trước khi xảy ra tổn thương nghiêm trọng)
  - Tính trọn vẹn: IDS không được bỏ qua xâm nhập trái phép nào (false negative). Đây là một điều kiện khó có thể thỏa mãn được.
  - Chịu lỗi (Fault Tolerance): yêu cầu bản thân IDS phải có khả năng chống lại tấn công.
  - Khả năng mở rộng (Scalability)



Một hệ thống hệ IDS

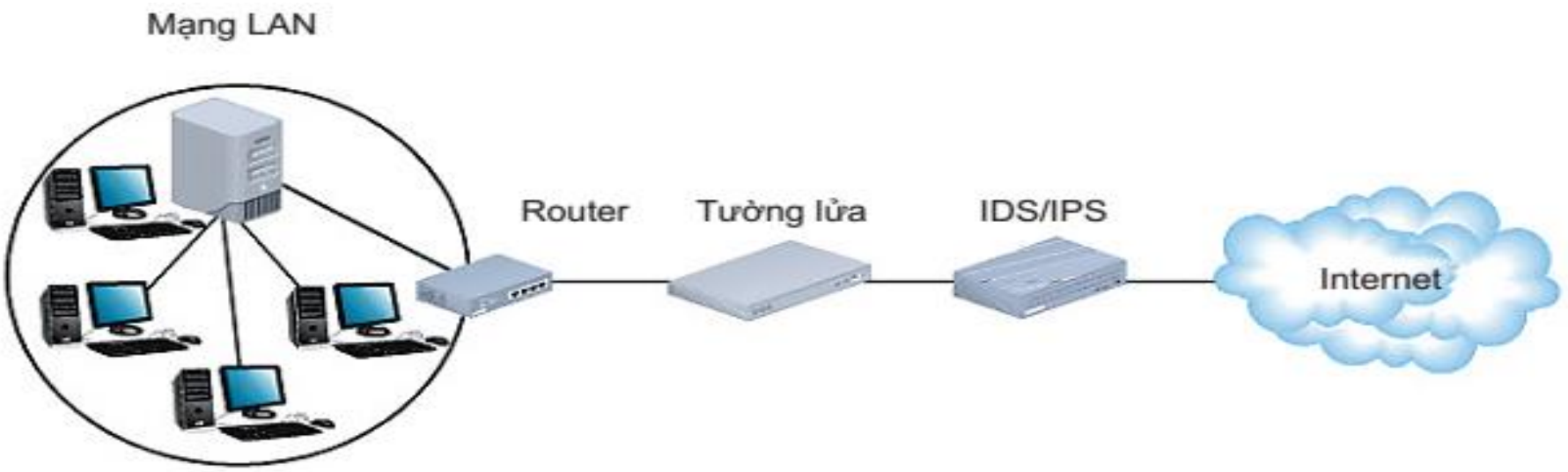


Các thành phần chính của một hệ IDS

IPS

- Mặc dù một IDS chỉ có thể phát hiện và ghi lại hoạt động đáng ngờ, một **IPS** (**instrusion-prevention system - hệ thống ngăn ngừa xâm nhập**) có thể phản ứng khi có cảnh báo về hoạt động đó.
- Ví dụ, nếu một hacker cố gắng gửi một lưu lượng làm ngập mạng, IPS có thể phát hiện nguy cơ này và ngăn chặn lưu lượng truy cập vào mạng dựa trên địa chỉ IP nguồn.
- -> cô lập, và IPS tiếp tục cho phép lưu lượng hợp lệ đi qua.
  - NIPS (network-based intrusion prevention - ngăn ngừa xâm nhập theo mạng)
  - HIPS (host-based intrusion prevention - ngăn ngừa xâm nhập theo máy).

Vị trí của IDS/IPS trên mạng



Công cụ quét

- Mặc dù đã nỗ lực hết sức để bảo vệ mạng với danh sách truy cập router, IDS/ IPS, tường lửa, server ủy nhiệm: vẫn có thể bỏ sót một vài lỗ hổng nguy hiểm.
- Để đảm bảo an toàn 1 cách triệt để, nên suy nghĩ giống hacker.
- để xác định các lỗ hổng trong kiến trúc bảo mật. Các công cụ quét là một cách đơn giản và hiệu quả để hacker – và bạn tìm ra các thông tin quan trọng về mạng :
  - Các host hiện có
    - Các dịch vụ (bao gồm cả các ứng dụng và các phiên bản) đang chạy trên mỗi host
    - Các hệ điều hành đang chạy trên mỗi host
    - Các cổng mở, đóng và được lọc trên mỗi host
    - Sự tồn tại của tường lửa và loại tường lửa
    - Các cấu hình phần mềm
    - Dữ liệu nhạy cảm và không được mã hóa

Công cụ quét

- **NMAP (Network Mapper)**

  NMAP có thể chạy trên hầu hết các hệ điều hành hiện nay, bạn có thể tải NMAP từ trang web *www.nmap.com*
- **Nessus** của Tenable Security, có thể thực hiện quét phức tạp hơn so với NMAP.
  - Ngoài các thông tin trên, Nessus có thể xác định được các dữ liệu nhạy cảm, không được mã hóa như số thẻ tín dụng được lưu trên các host trong mạng của bạn.
- Một công cụ kiểm thử chuyên sâu khác là **metasploit**,
  - Công cụ này kết hợp các kỹ thuật quét và khai thác đã biết để đưa ra các kết hợp mới.

Bẫy nhử - Honeypot

- Muốn tìm hiểu thêm về kỹ thuật lấy tin của hacker -> tạo ra một **honeypot** hoặc thiết kế một hệ thống cố tình tạo ra lỗ hổng cho hacker khai thác.
- Khi hacker xâm nhập vào honeypot, quản trị mạng có thể sử dụng một phần mềm theo dõi hoặc các nhật ký truy cập để lần theo dấu vết của hacker.
  - Quản trị mạng có thể biết thêm về các lỗ hổng cần phải được giải quyết trong mạng thật.
- Honeypot phải được tách biệt với hệ thống bảo mật, tránh hacker sử dụng nó như một host trung gian để thực hiện các cuộc tấn công khác.

NAT/PAT

- Quá trình chuyển đổi địa chỉ mạng (NAT)
  Cho phép sử dụng các địa chỉ IP riêng trên mạng Internet
  Thay thế địa chỉ IP cá nhân bằng địa chỉ public
- Chuyển đổi địa chỉ cổng (PAT)
  Biến thể của NAT
  Các gói tin gửi đi có cùng địa chỉ IP nhưng # về số cổng TCP
- Các ưu điểm của NAT
  Che dấu địa chỉ IP của các thiết bị trong nội bộ
  Cho phép nhiều thiết bị chia sẻ chung một số ít các địa chỉ IP public
- Điều khiển truy cập mạng (NAC)
  Kiểm tra trạng thái hiện tại của hệ thống hay thiết bịmạng:
  Trước khi cho phép kết nối mạng, Thiết bị phải đáp ứng một tập tiêu chuẩn
  Nếu không đáp ứng, NAC sẽ cho phép client kết nối tới một mạng cách ly, cho tới khi các thiếu sót được khắc phục

3.4 Bảo mật máy chủ và máy trạm

- Tăng cường hệ điều hành
  - HDH mới chưa được thăm dò ồ ạt của tin tặc -> đáng tin cậy
  - Có những tính năng quan trọng gồm khả năng hỗ trợ, các biện pháp chịu đựng lỗi UPS, đĩa RAID, logging, và kiểm soát truy cập
- Ba thủ tục:
  - Xóa các chương trình, các dịch vụ, các quá trình không cần thiết
  - Cập nhật tất cả các chương trình, các dịch vụ
  - Tối thiểu hóa các thông tin phổ biến về HĐH, dịch vụ, các khả năng của hệ thống
- Tạo đường cơ sở cho phần mềm máy chủ
  - Đường cơ sở: tiêu chuẩn kiểm tra để đánh giá hệ thống
  - Các thiết lập cấu hình được áp dụng cho từng máy tính trong tổ chức
  - Chính sách bảo mật xác định phải bảo vệ cái gì, đường cơ sở xác định bảo vệ như thế nào?

Bảo mật phần mềm hệ điều hành

- Cấu hình bảo mật hệ điều hành (HĐH) và các cài đặt HĐH hiện tại có hàng trăm thiết lập bảo mật khác nhau, có thể sử dụng để điều chỉnh cho phù hợp với đường cơ sở.
- Cấu hình đường cơ sở tiêu biểu
  - Thay đổi các thiết lập mặc định không an toàn
  - Loại bỏ các phần mềm, dịch vụ, giao thức không cần thiết (được cài đặt theo mặc định)
  - Kích hoạt các chức năng bảo mật, ví dụ như tường lửa
- Thực thi việc quản lý các bản vá
  - Người dùng không biết sự tồn tại của các bản vá hay vị trí để lấy được các bản vá
  - Các hệ điều hành hiện nay đều có khả năng tự động thực hiện cập nhật
  - Đôi khi các bản vá có thể làm nảy sinh những vấn đề mới

Bảo mật phần mềm hệ điều hành

- Yêu cầu xác thực mạnh mẽ để truy cập từ xa và từ nội bộ.
- Quản lý chặt chẽ người dùng và các nhóm để kiểm soát các quyền không thích hợp.
- Cài đặt và cấu hình hệ thống tập tin: Cấu hình Access Control Lists (ACL) để loại bỏ quyền mạnh mẽ và không thích hợp
- Chỉ cài đặt phần mềm đã thử nghiệm và được phê duyệt.
- Áp dụng tất cả bản sữa chữa (hot-fixes), bản vá lỗi (patches) và gói dịch vụ (and service packs) có liên quan

Bảo mật bằng phần mềm chống phần mềm độc hại

- Các phần mềm chống phần mềm độc hại của bên thứ ba có thể cung cấp thêm sự bảo mật, bao gồm:
  - Phần mềm chống vi rút
  - Phần mềm chống thư rác
  - Phần mềm phong tỏa pop-up
  - Tường lửa dựa trên máy chủ

Phần mềm diệt vi rút

- Phần mềm diệt virus
  - Phần mềm kiểm tra một máy tính có bị tiêm nhiễm virus hay không
  - Quét các tài liệu mới có thể chứa virus
  - Tìm kiếm các mẫu virus đã được biết trước
- Nhược điểm của phần mềm diệt virus
  - Nhà cung cấp phải liên tục tìm các virus mới, cập nhật và phân phối các file chữ ký (signature file) tới người dùng
- Phương pháp khác: giả lập mã (code emulation)
  - Các mã khả nghi được thực thi trong một môi trường ảo

Phần mềm chống thư rác

- Những kẻ gửi thư rác có thể phát tán phần mềm độc hại thông qua các thư điện tử có file đính kèm
- Thư rác có thể được sử dụng trong các cuộc tấn công dùng kỹ nghệ xã hội
- Các phương thức lọc thư rác

Lọc Bayesian

Lọc trên máy chủ cục bộ

Danh sách đen Danh sách trắng

Chặn các kiểu file đính kèm khả nghi

Phần mềm phong tỏa pop-up

Pop-up

Một cửa sổ xuất hiện trên Web site Thường do các nhà quảng cáo tạo ra

Phần mềm phong tỏa pop-up

Một chương trình riêng biệt, giống như một phần của gói phần mềm chống phần mềm gián điệp

Được tích hợp vào trong trình duyệt

Cho phép người dùng hạn chế hoặc ngăn chặn hầu hết các cửa sổ pop-up

Có thể hiển thị cảnh báo trong trình duyệt

Cho phép người dùng có thể lựa chọn để hiển thị pop-up

Tường lửa dựa trên máy chủ

Tường lửa (firewall)

- Được thiết kế nhằm ngăn chặn các gói tin độc hại truy cập hoặc gửi đi từ máy tính
- Có thể dựa trên phần cứng hoặc phần mềm
- Phần mềm tường lửa dựa trên máy chủ hoạt động trên hệ thống cục bộ

Tường lửa trong Microsoft Windows 7

- Ba kiểu thiết lập dành cho các mạng: public, home, hoặc work
- Người dùng có thể cấu hình các thiết lập riêng cho từng kiểu mạng

3.5 Các thiết bị di động

- PDAs, Cellphone, Smartphone
- WAP security:
  - Đăng nhập vô danh
  - Server xác thực: workstation xác thực lại server
  - Xác thực hai chiều: server client
- Smartphone, máy tính bảng đã trở thành kho chứa thông tin cá nhân nhạy cảm
- Dễ mất, thất lạc, bị lấy cắp, bị kẻ xấu lợi dụng thu thập thông tin cá nhân nhạy cảm, làm cầu nối tấn công mạng doanh nghiệp

iOS/Android Malware

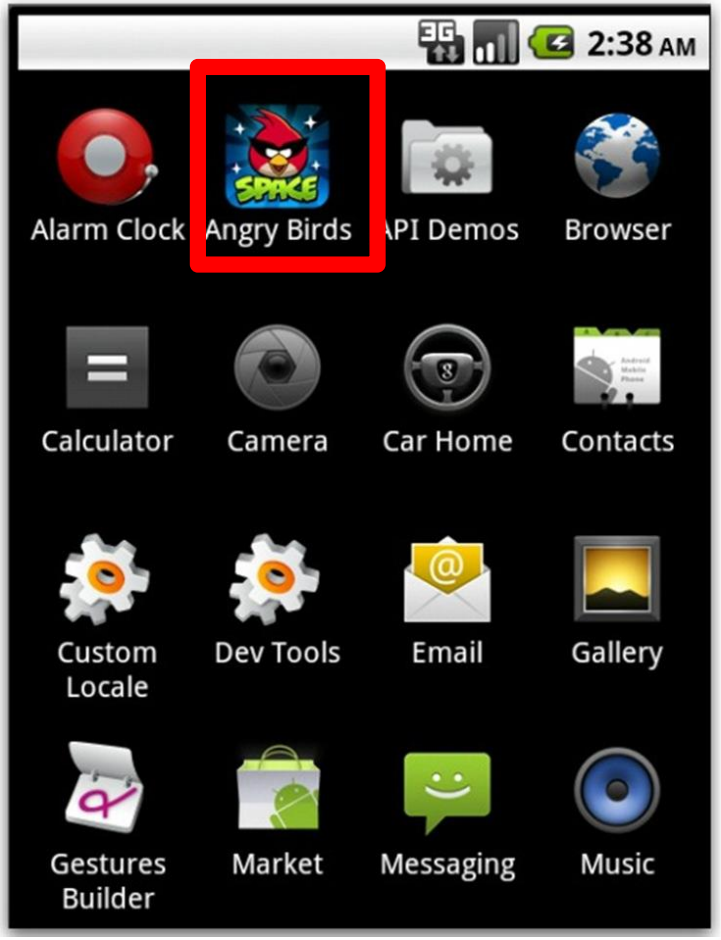
- iOS malware: ít
- Juniper Networks: chủ yếu tăng số lượng Android malware từ 2010 đến nay
- Các loại:
  - Trojans
  - Monitoring apps/spyware
  - Adware
  - Botnets

Android: DroidDream Malware

- Ảnh hưởng 58 apps trên Android Market, March 2011
- 260,000 downloads trong 4 days
- Cách thức:
  - Rooted phone via Android Debug Bridge (adb) vulnerability
  - Sent premium-rate SMS messages at night ($$$)
- Google xóa các app sau 4 ngày release, Khóa 3 developers

Android: Fake *Angry Birds Space*

- Bot, Trojan
- Masquerades as game
- Roots Android 2.3 devices using "Gingerbreak" exploit
- Device joins botnet



Android: Google Wallet Vulnerabilities

- Google Wallet cho phép thanh toán điện tử
  - Sử dụng NFC technology
- Thông tin credit card được lưu giữ an toàn
  - Separate chip, SD card, SIM card
- Tuy nhiên một số thông tin khác không được lưu giữ an toàn

Những biện pháp bảo vệ

- 1. Không hack thiết bị (jailbreak với iOS / root với Android). Chỉ cài ứng dụng từ nguồn đáng tin cậy.
  - Những ứng dụng miễn phí có tính năng hấp dẫn, nhưng xuất phát từ nguồn thiếu tin cậy/ không được kiểm duyệt nên tiềm ẩn nguy cơ chứa mã độc
- 2. Thiết lập chế độ khóa thiết bị và đặt thời gian tự động khóa màn hình.
- 3. Tắt Wi-Fi, Bluetooth, NFC, dịch vụ địa điểm nếu không dùng.
- 4. Khi thực hiện giao dịch tài chính, ngân hàng, mua bán trực tuyến: tránh dùng mạng Wi-Fi công cộng; chắc chắn địa chỉ web là chính xác; thoát ngay (logout) thay vì chỉ đóng trình duyệt khi kết thúc sử dụng dịch vụ;
- 5. Không ghi nhớ tên tài khoản người dùng và mật mã trong trình duyệt .

3.6 Bảo mật các kết nối internet

- Email
- Port, Socket
- Web
  - SSL/TLS
  - HTTPS
  - Add-in:
    - Javascript
    - Java Applet
    - ActiveX Control
    - CGI
    - Buffer Overflow
    - Cookies

Bảo mật gửi email

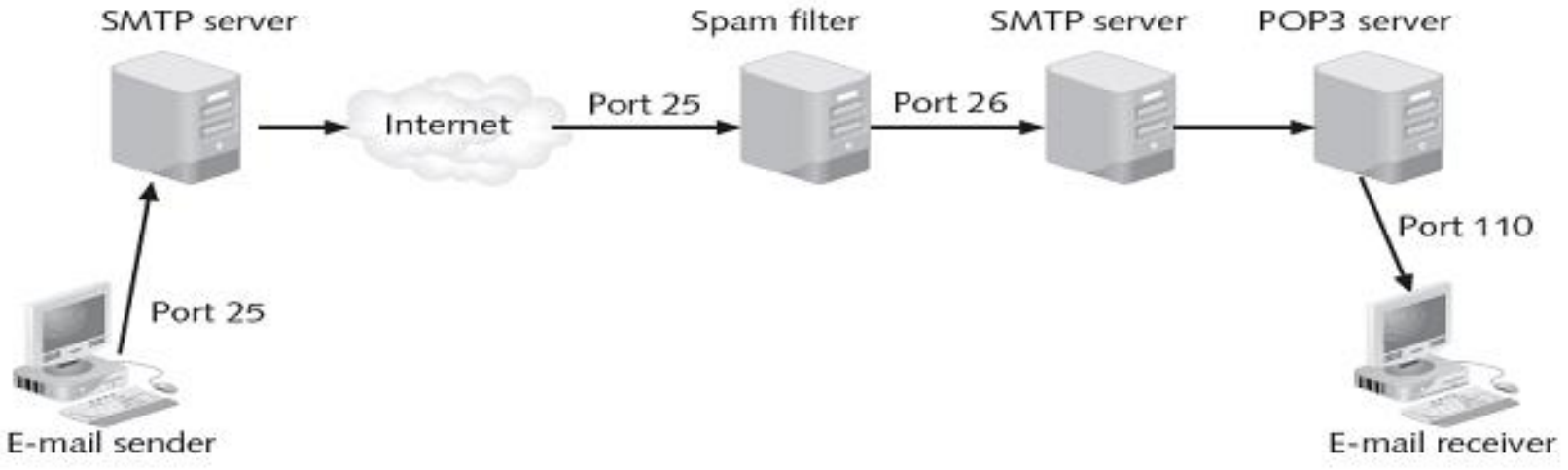
- Trên thực thế, một số giao tiếp qua email là rất không an toàn.
- Phụ thuộc vào mail server và client, các tin nhắn có thể được gửi đi mà không hề được mã hóa,
- Có thể được đọc bởi bất kỳ người nào có khả năng thu được tin nhắn trên đường truyền đến người nhận.
- Thêm vào đó, một người dùng với ý định gây hại có thể dễ dàng giả mạo anh ta là một người khác.
- Ví dụ, nếu địa chỉ emailcủa bạn là *joe@example.com:*
  - Một người khác có thể giả mạo địa chỉ email của bạn và gửi tin nhắn, giống như được gửi từ *joe@example.com*

Bảo mật gửi email

- Chương trình **PGP (Pretty Good Privacy)** là một hệ thống mã hóa khóa công khai, có thể xác nhận việc xác thực người gửi email và mã hóa dữ liệu email trong quá trình truyền tải.
- PGP hiện nay đang được quản lý tại MIT, và có thể được sử dụng miễn phí cả trong các gói phần mềm mã nguồn mở và thương mại.
- Kể từ khi phát hành, nó đã trở thành công cụ phổ biến nhất để mã hóa e-mail.

Bộ lọc thư rác

- Các bộ lọc thư rác được cài đặt với máy chủ SMTP
- Bộ lọc được cấu hình để "nghe ngóng" tại cổng 25
- Những thư điện tử không phải thư rác được chuyển tới máy chủ SMTP đang "nghe ngóng" tại một cổng khác
- Phương pháp ngăn không cho máy chủ SMTP gửi lại thông báo cho kẻ gửi thư rác biết việc phân phát thư rác bị thất bại



Bộ lọc thư rác

- Bộ lọc thư rác được cài đặt trên máy chủ POP 3
  Trước tiên, tất cả thư rác phải truyền qua máy chủ SMTP, sau đó chúng được chuyển tới hộp thư của người dùng
  Có thể làm tăng chi phí
  Lưu trữ, truyền dẫn, sao lưu, xóa hủy
- Lọc thư rác thông qua hợp đồng với một đối tác thứ ba
  Tất cả thư điện tử được đi qua một bộ lọc thư rác từ xa của đối tác thứ ba
  Thư điện tử được "làm sạch" trước khi chuyển tiếp tới tổ chức

SSL (Secure Sockets Layer)

- **SSL** là một phương pháp mã hóa các quá trình truyền tin TCP/IP – bao gồm các trang web và dữ liệu được nhập vào Web form - trên đường đi giữa client và server
- Sử dụng kỹ thuật mã hóa khóa công khai.
- Ví dụ mua bán chứng khoán hoặc mua hàng trên mạng: sử dụng SSL để truyền thông tin về đơn hàng.
- SSL rất phổ biến và được sử dụng rộng rãi.
- Trang web HTTP: yêu cầu được xử lý bằng giao thức HTTP thông qua cổng 80 trong TCP/IP.
- Trang web bắt đầu bằng **HTTPS** (**HTTP over Secure Sockets Layer**): sẽ yêu cầu dữ liệu được truyền giữa server và client phải sử dụng mã hóa SSL.
- HTTPS sử dụng cổng 443 của giao thức TCP

SSL

- Mỗi lần thiết lập một kết nối SSL, client và server sẽ thiết lập **phiên làm việc SSL (SSL session)** riêng,
- Hoặc một kết nối giữa client và server được được xác định bởi một thỏa thuận về một tập các kỹ thuật mã hóa xác định.
- Một phiên làm việc SSL cho phép client và server liên tục trao đổi dữ liệu một cách an toàn với nhau miễn là client vẫn kết nối với server.
- Một phiên giao dịch được tạo ra bởi giao thức bắt tay SSL
- Webserver có thể chọn để gửi cho trình duyệt của Client một khóa công khai hoặc một chứng thư số.
- Sau khi client và server đã đồng ý về các điều khoản mã hóa, chúng bắt đầu trao đổi dữ liệu

TLS

- SSL ban đầu được phát triển bởi Netscape.
- Sau đó đã cố gắng để chuẩn hóa SSL trong một giao thức gọi là **TLS (Transport Layer Security - Giao thức bảo mật tầng Giao vận**).
- Giao thức TLS, được hỗ trợ bởi các trình duyệt web hiện đại, sử dụng các thuật toán mã hóa hơi khác so với SSL, nhưng còn lại thì rất giống với phiên bản mới nhất của SSL.

Các điểm yếu của Web Client

- JavaScript
- Cookies
- Applets

JavaScript

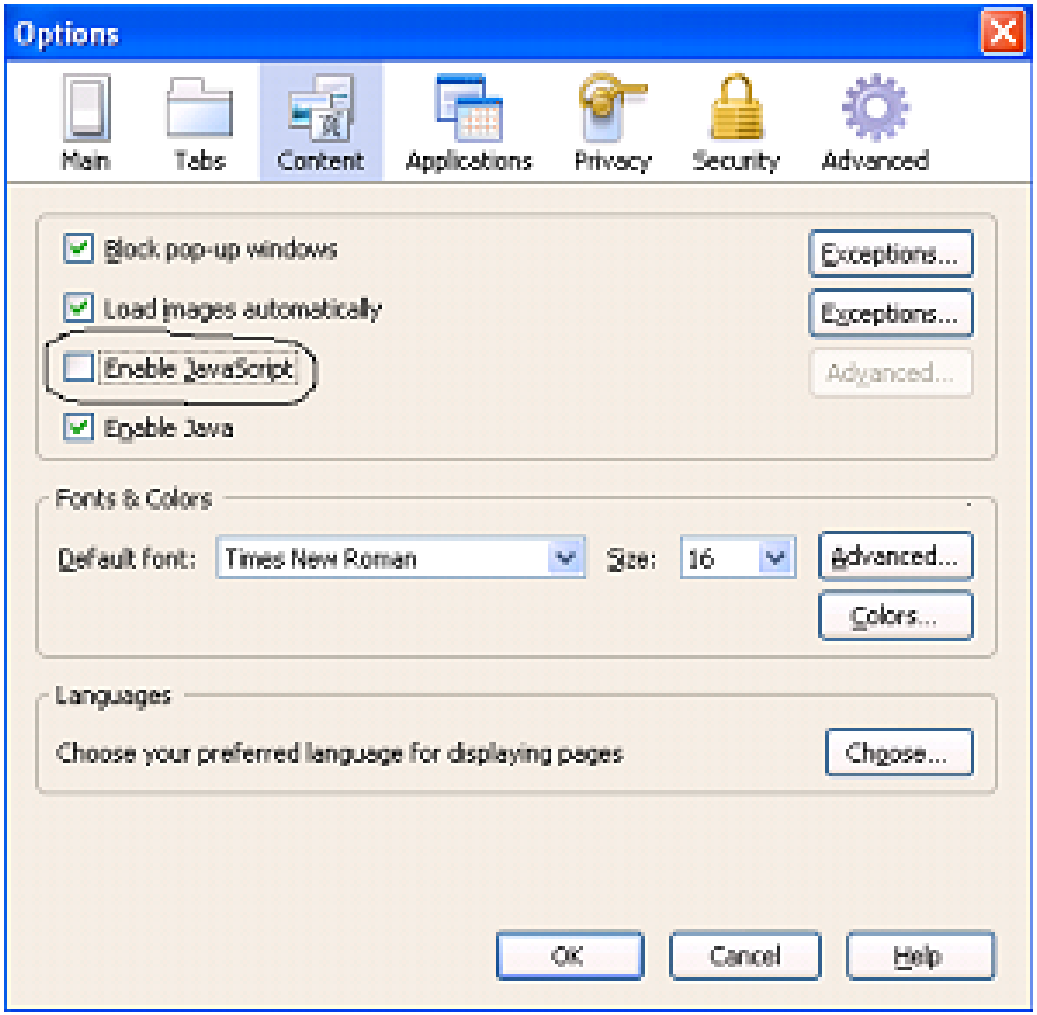
- Các nguy cơ:
  - Ăn trộm địa chỉ Email
  - Ăn trộm thông tin người sử dụng
  - Kill một số tiến trình
  - Chiếm tài nguyên CPU và bộ nhớ
  - Shutdown hệ thống
  - Relay email để phục vụ cho gửi spam
  - Phục vụ cho việc chiếm đoạt website

JavaScript

- Các biện pháp phòng chống

- Disable chức năng chạy JavaScript trong trình duyệt.

- Thường xuyên cập nhập phiên bản mới của trình duyệt
- Kiểm tra kỹ mã lệnh của web Server



Cookies

- File cookies lưu trữ một số các thông tin cá nhân của người dùng:
  – Số thẻ tín dụng
  – Username/Password
- Có thế sử dụng chung cho nhiều website khác nhau
- Trình duyệt có thể cho phép web server lưu trữ thông tin trên đó

Cookies

- Các nguy cơ:
  – Kẻ tấn công có thể sử dụng Telnet để gửi các dạng cookies mà chúng muốn để đánh lừa web server.
  – Kẻ tấn công có thể lợi dụng cookies để lấy trộm các thông tin về người dùng, về tổ chức và câu hình Security của mạng nội bộ
  – Kẻ tấn công có thể lợi dụng lỗi Script Injection để cài các script nguy hiểm lên hệ thống nhằm chuyển các cookies về hệ thống thay vì phải chuyển lên web server

Cookies

- Các biện pháp phòng chống:
  – Disable Cookies trên trình duyệt web
  – Sử dụng những trình xóa cookies không cần thiết
  – Cấu hình web server không được "tin tưởng" vào các cookies dạng yêu cầu cung cấp thông tin, yêu cầu điều khiển hoặc yêu cầu dịch vụ.. Được lưu ở client
  – Không lưu trữ các thông tin nhạy cảm trên cookies
  – Sử dụng SSL/TLS

Applets

- Là những chương trình Java nhỏ, có thể thực thi trên các trình duyệt.
- Java Applets chạy trên những client dựa vào Java Virtual Machine (VM) được hầu hết các hệ điều hành hỗ trợ.

Applets

- Các nguy cơ:
  – Các chương trình Applets có thể truy cập các tài nguyên hệ thống
  – Có thể sử dụng để giả mạo chữ ký
  – Có thể dùng để cài đặt Virus, Trojan, worm
  – Có thể sử dụng tài nguyên mạng để tấn công, thăm dò hệ thống mạng khác.
- Các biện pháp phòng chống:
  – Không sử dụng Applets, tắt hỗ trợ Java trên các trình duyệt
  – Tuyên truyền, hướng dẫn người sử dụng

SSH (Secure Shell – Shell bảo mật)

- Telnet: cấu hình từ xa đến router. Tuy nhiên, telnet cung cấp bảo mật kém cho việc thiết lập một kết nối (xác thực) và không mã hóa truyền dữ liệu
- **SSH** là một tập các giao thức để làm cả hai việc này:
- Đăng nhập an toàn vào một server, thực hiện lệnh trên server đó, và sao chép các fie đến hoặc từ máy đó.
- SSH mã hóa dữ liệu trao đổi trong suốt phiên giao dịch.
- Nó bảo vệ chống lại một số mối đe dọa an ninh:
  - Truy cập trái phép vào server
  - Giả mạo IP
  - Chặn các dữ liệu trong quá trình truyền
  - **Giả mạo DNS (DNS spoofig)**, trong đó một hacker giả mạo các bản ghi name server để làm sai lệch định danh của host.
- Tùy theo phiên bản, SSH có thể sử dụng thuật toán DES, 3DES, RSA, Kerberos

FTP - SFTP

- FTP
  - Anymnomous
  - Secure FTP: sử dụng giao thức SSH (secure shell)
  - Sharing Files

FTP

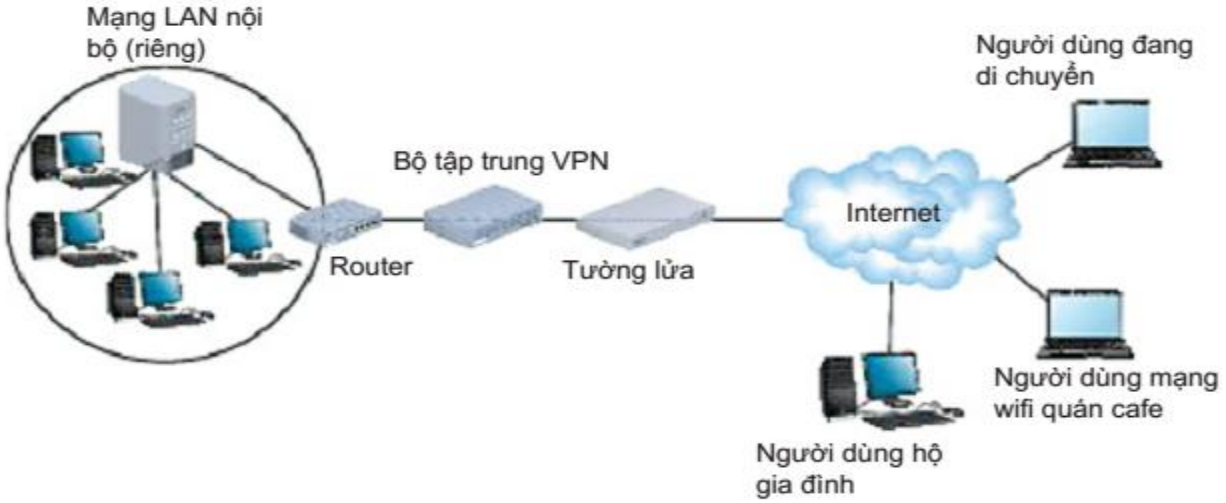
- Các giao thức TCP/IP được sử dụng để truyền file
  Giao thức truyền file (FTP)
  Giao thức sao lưu an toàn (SCP)
- Các phương pháp sử dụng giao thức FTP trên máy chủ cục bộ
  Từ dấu nhắc lệnh (command prompt)
  Sử dụng trình duyệt Web (Web browser)
  Sử dụng trình khách FTP (FTP client)
- Sử dụng FTP phía sau tường lửa có thể ngăn chặn được nhiều thử thách
  Chế độ FTP chủ động (active mode)
  Chế độ FTP thụ động (passive mode)

FTP

- Các lỗ hổng của giao thức FTP
  - FTP không sử dụng mật mã
  - Các file được truyền bởi FTP là lỗ hổng đối với các vụ tấn công kẻ đứng giữa (man-in-the-middle)
- Các tùy chọn truyền file bảo mật thay thế FTP
  - FTP sử dụng tầng kết nối an toàn bảo mật (FTP using Secure Sockets Layer - FTPS)
  - FTP an toàn (Secure FTP - SFTP)

IPSec (Internet Protocol Security)

- Giao thức **IPSec** định nghĩa việc mã hóa, xác thực, và quản lý khóa trong truyền thông TCP/IP.
- IPSec là một sự tăng cường cho IPv4 và là mặc định cho IPv6.
- IPSec hoạt động ở tầng Mạng của mô hình OSI.
- IPSec có thể được sử dụng với bất kỳ loại truyền dữ liệu TCP/IP nào. Tuy nhiên, nó thường chạy trên router hoặc các thiết bị kết nối khác trong mạng VPN



Giao thức CHAP

- **Giao thức CHAP** (Challenge Handshake Authentication Protocol) Giao thức xác thực thử thách-bắt tay CHAP là một giao thức xác thực dựa trên PPP(điểm – điểm)
- CHAP mã hóa tên đăng nhập và mật khẩu trong quá trình truyền tải.
- Đòi hỏi các bước để hoàn tất quá trình xác thực: **bắt tay ba bước (three-way handshake)**.

Hình 4-12 **Bắt tay ba bước sử dụng trong CHAP**