Chương 3

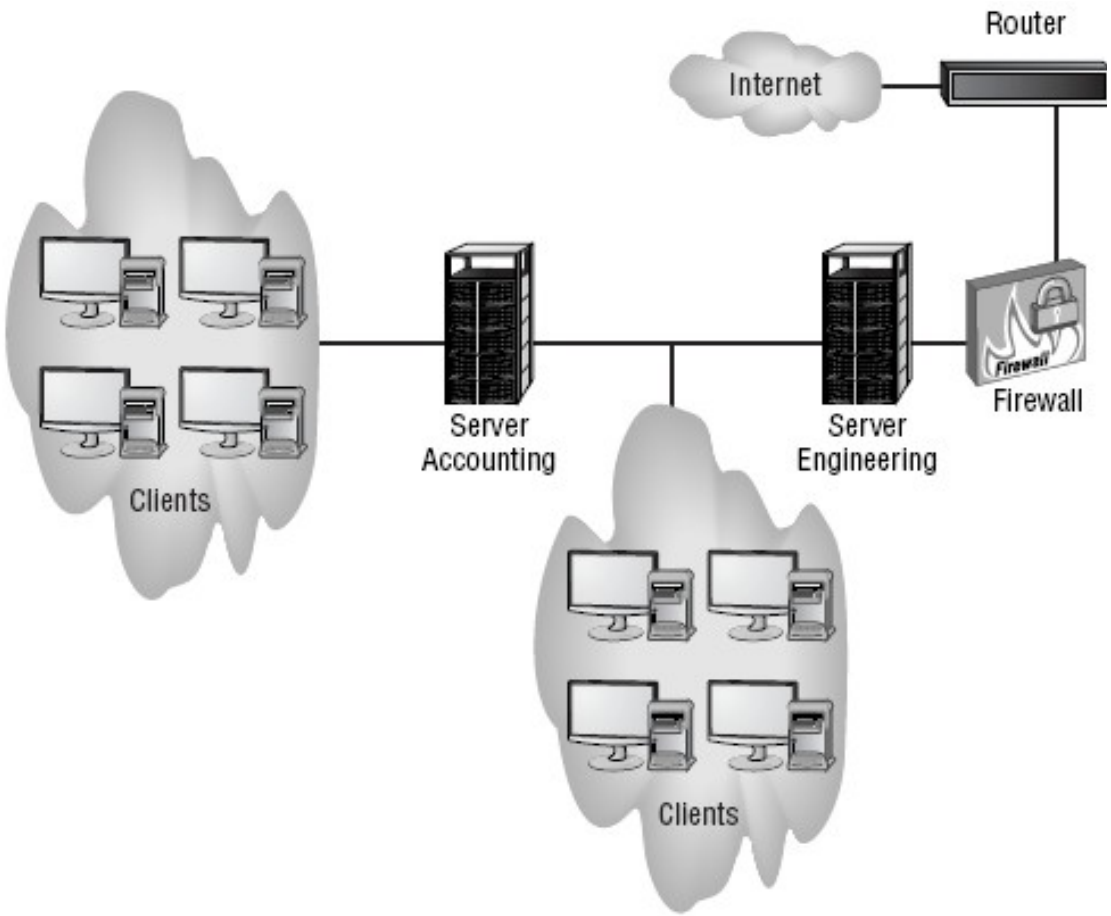
Hạ tầng cơ sở và kết nối

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

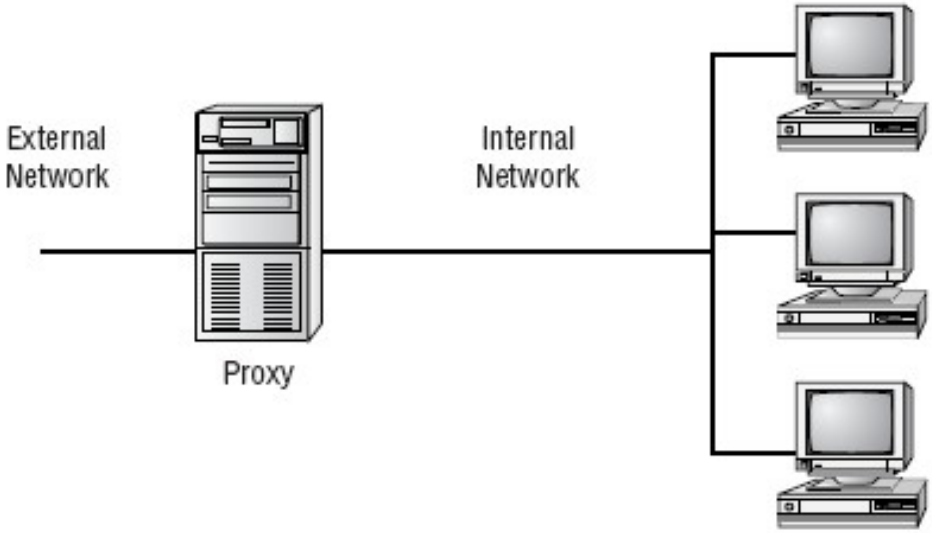
- Liên quan đến khía cạnh cơ bản nhất của dòng thông tin và cách làm việc trong hệ thống mạng.
- Cơ sở hạ tầng là nền tảng cho tất cả các công việc trong tổ chức
- Các thiết bị:
  - Router
  - Firewall
  - Switch
  - Server
  - Workstation


Router
Internet
Clients
Server
Accounting
Server
Engineering
Firewall
Firewall
Clients

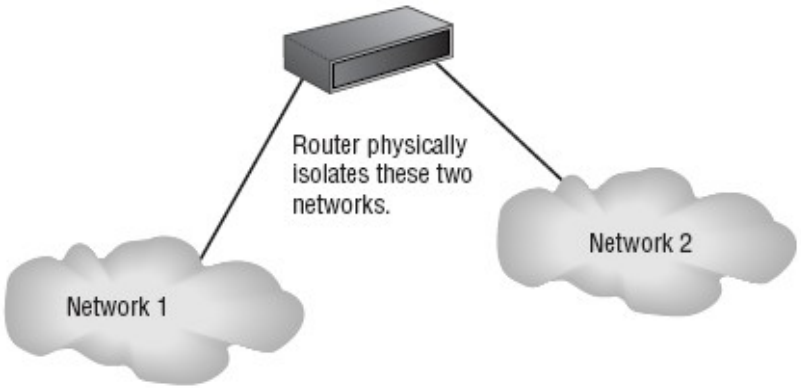
- Thành phần phần mềm
  - Nhiều hệ thống làm việc độc lập
  - Cần có một trung tâm điều hành quản lý chung NOC (Network Operator Center)

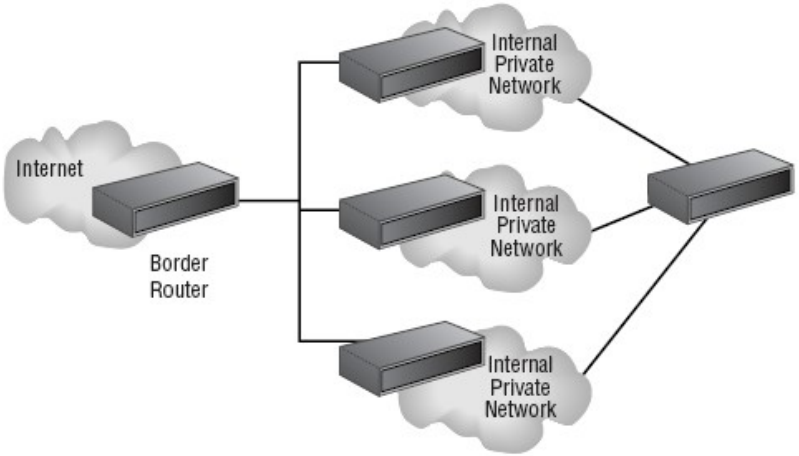
3.2 Các thiết bị nền tảng

- Firewall
  - Packet filter
  - Proxy firewall
  - Stateful inspection

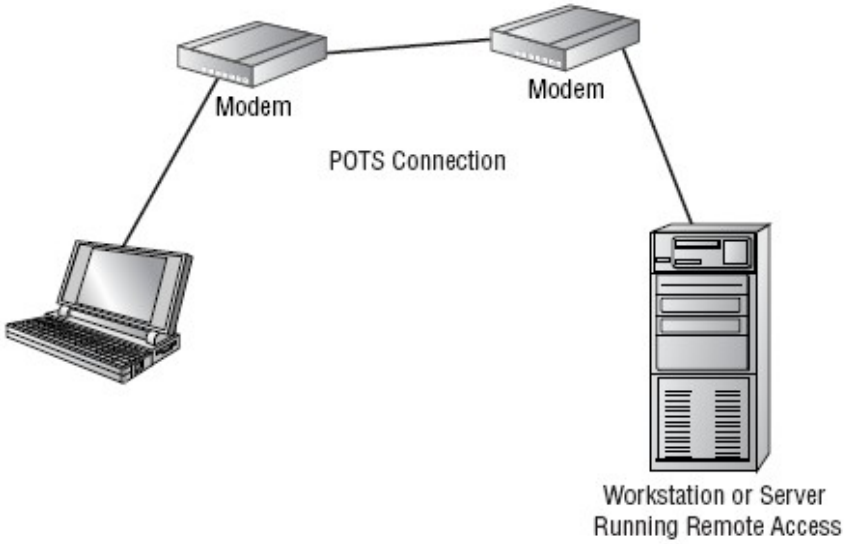


- Hub
- Router


Router physically isolates these two networks.
Network 1
Network 2


Internet
Border Router
Internal Private Network
Internal Private Network
Internal Private Network

- 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:
  - Phần mềm chạy trên workstation hoặc thiết bị mạng kiểm tra và theo dõi các hoạt động mạng
  - Có thể cấu hình alarm, phân tích đánh giá log,…
  - Được bán kèm với firewall.

3.4 Bảo mật máy chủ và máy trạm

- Tăng cường hệ điều hành
- 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

3.5 Các thiết bị di động

- PDAs, Cellphone
- WAP security:
  - Đăng nhập vô danh
  - Server xác thực: workstation xác thực lại server
  - Xác thực hai chiều: server client

3.6 Bảo mật các kết nối internet

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

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