Bảo mật mạng máy tính

- ✓ Khái niệm & mục đích bảo mật
- ✓ Mục tiêu tấn công
- ✓ Cách thức tấn công
- ✓ Công nghệ bảo mật

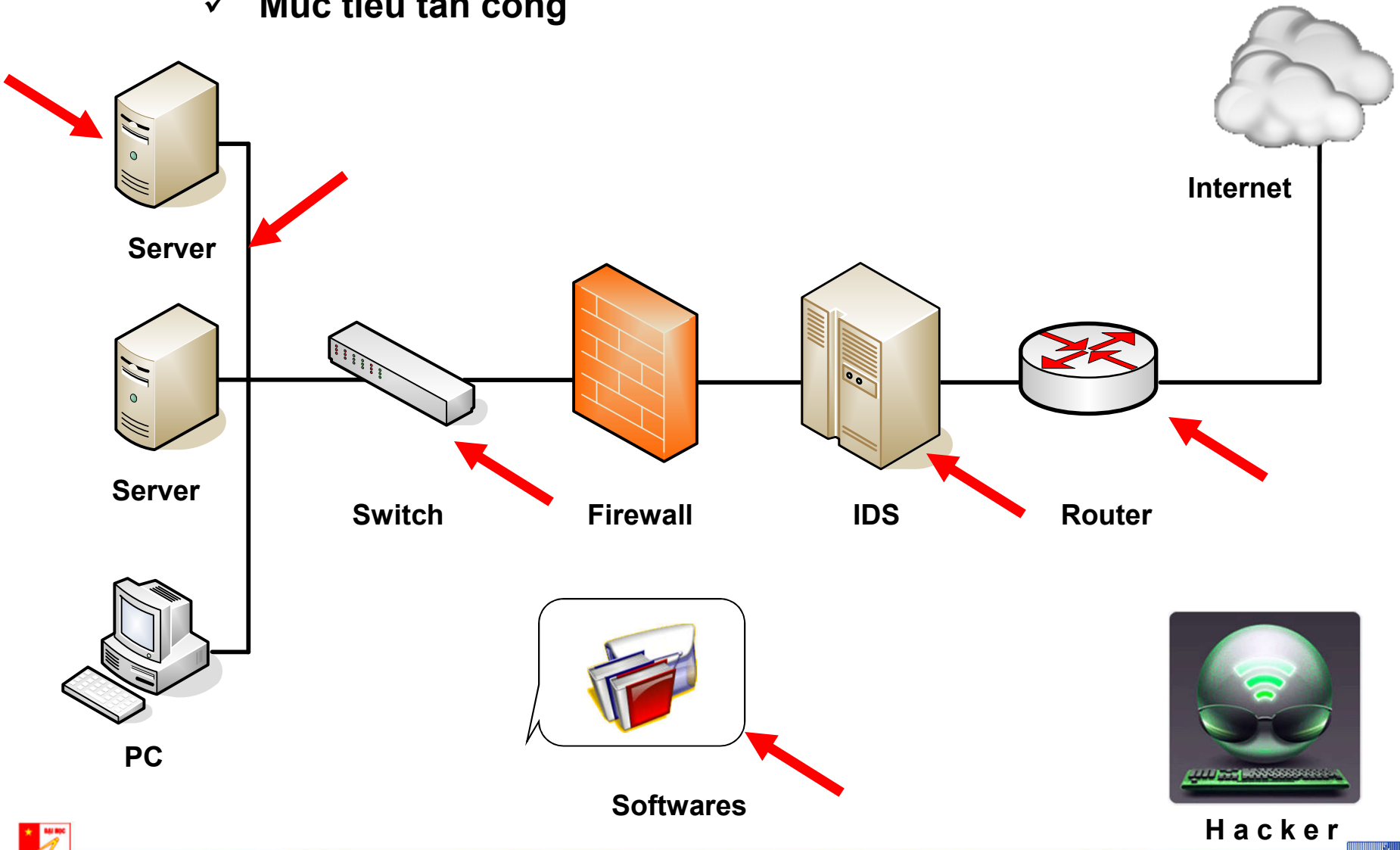
Hệ thống Firewall

- ✓ Định nghĩa
- ✓ Hoạt động
- ✓ Phân loại
- ✓ Mô hình tường lửa

Mô phỏng Packet Filtering Firewalls

- ✓ **Khái niệm**
  - o Bảo vệ các dữ liệu, tài nguyên, cơ sở hạ tầng mạng
    - ▪ Kẻ xấu
    - ▪ Từ chối dịch vụ
    - ▪ Sử dụng trái phép
  - o Dữ liệu: Tài liệu, công trình nghiên cứu,CSDL, thẻ…
  - o Tài nguyên: Máy tính, server, băng thông…
  - o Cơ sở hạ tầng mạng: Routers, switches, Cable …
- ✓ **Mục đích bảo mật**
  - o Hiệu quả
  - o Tin cậy
  - o Toàn vẹn

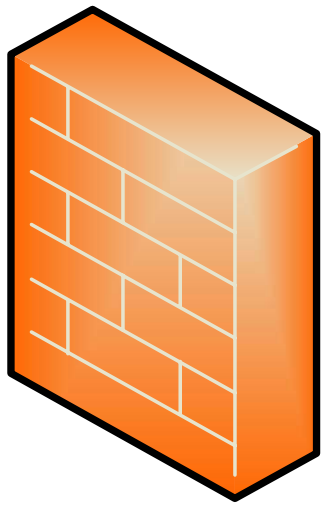
✓ Muc tiêu tấn công



- ✓ **Cách thức tấn công**
  - o Dos (Denial of Service)
  - o Tràn bộ đệm (Over Buffer)
  - o Dò tìm gói tin
  - o Giả mạo IP
  - o Tấn công mật khẩu
  - o Virus, Trojan….
- ✓ **Công nghệ bảo mật**
  - o Mật mã (encpytion)
  - o Tường lửa (firewalls)
  - o Công cụ giám sát (monitoring tool)
  - o Giả mạo IP (fake IP)
  - o Tấn công mật khẩu (password attack)
  - o Virus, Trojan….

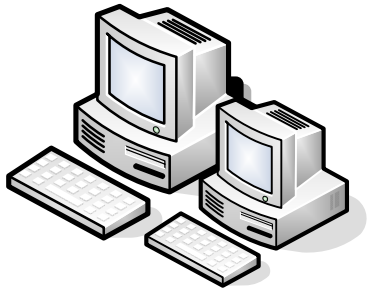
Firewall là gì?

- ✓ **Định nghĩa**
  - o Firewalls là hệ thống ngăn chặn việc truy nhập trái phép từ bên ngoài vào mạng
  - o Phần cứng, phần mềm hoặc kết hợp cả hai

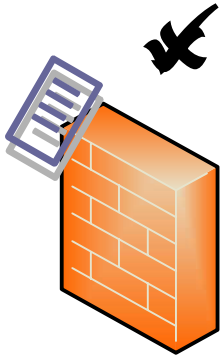


- ✓ **Chức năng** :
  - o Bảo vệ tài nguyên
  - o Kiểm soát truy cập
  - o Nâng cao hiệu suất
  - o Tự động hóa bảo vệ & cảnh báo

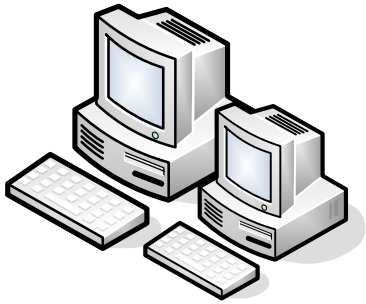
✓ Hoạt động



Mạng ngoài



Firewall

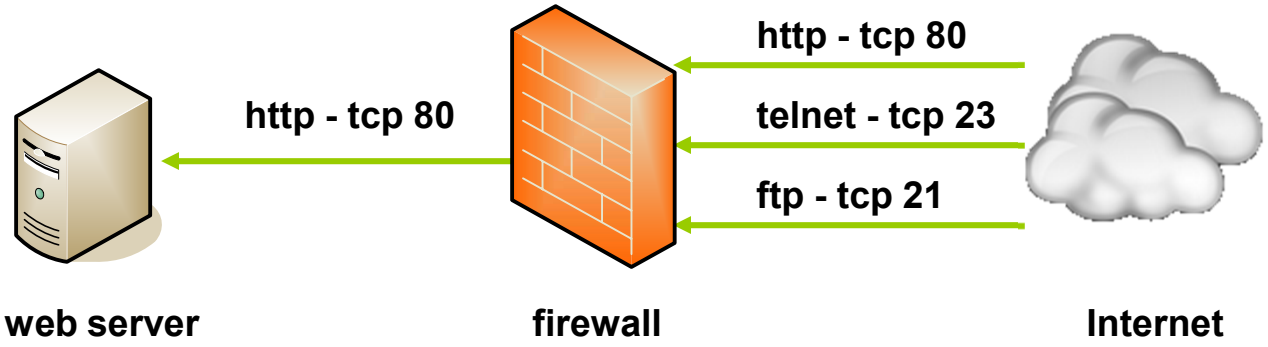


Mạng trong

✓ Phân loại firewall

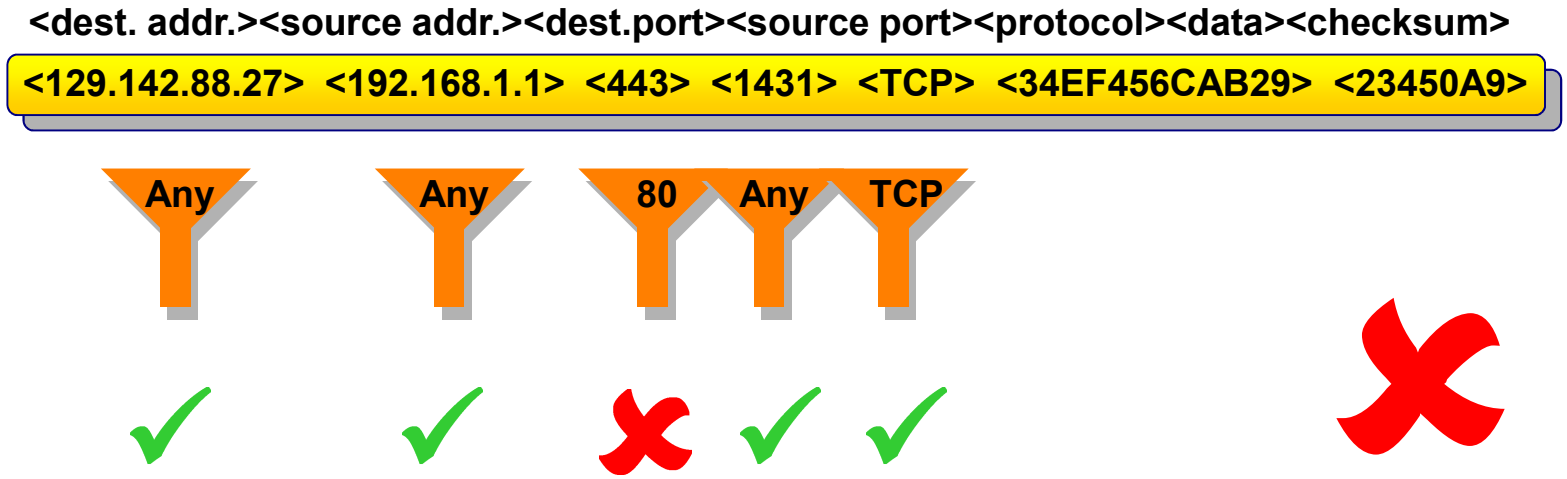
o Packet filtering firewalls

- Kiểm tra địa chỉ IP, cổng đích & nguồn hay kiểu giao thức của một gói tin, dựa vào quy luật để cho hay ko cho phép gói đó tin đi qua mạng

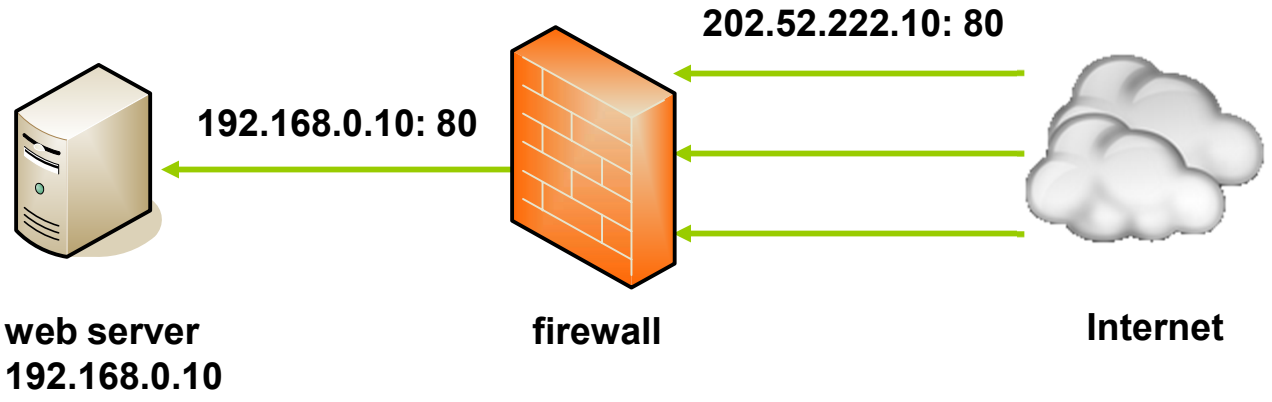


- **Chỉ cho phép http - tcp 80**
- **Chặn tất cả**

- Ví dụ: Một quy tắc chỉ cho phép gói IP nào dùng trình duyệt web (port 80) mới được phép đi qua

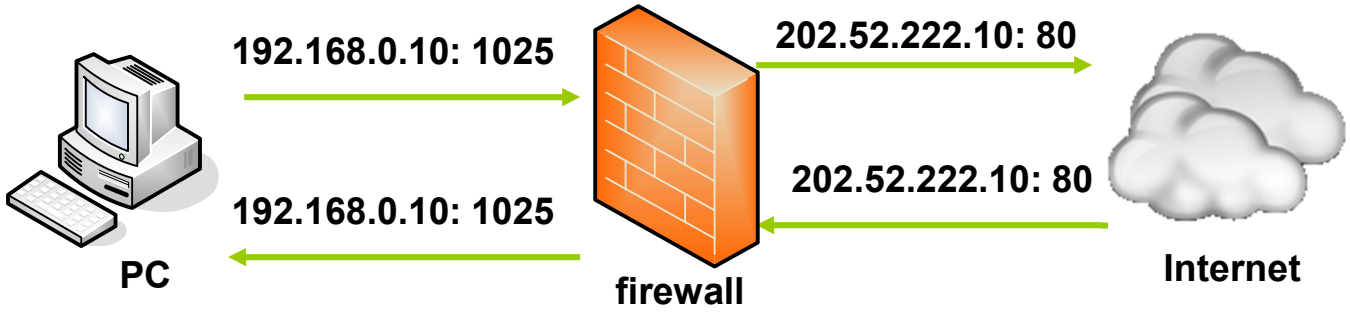


- **Application layer firewalls**
  - Được xem như một firewall ủy quyền, cổng ứng dụng
  - Proxy như một đại diện cho những ai dùng proxy đó, che dấu thông tin thực khi giao tiếp bên ngoài
  - Các gói yêu cầu truy nhập được sẽ được biên dịch tại firewall trước khi vào mạng trong



Dịch địa chỉ 202.52.222.10 : 80
thành 192.168.0.10 : 80

- **Stateful inspection firewalls**
  - Kiểm tra trạng thái và nội dung của gói
  - Ghi nhớ những yêu cầu đi ra và chỉ cho phép những yêu cầu đó trở lại qua Firewall
  - Việc cố tình truy cập vào mạng trong sẽ bị từ chối nếu bên trong không yêu cầu



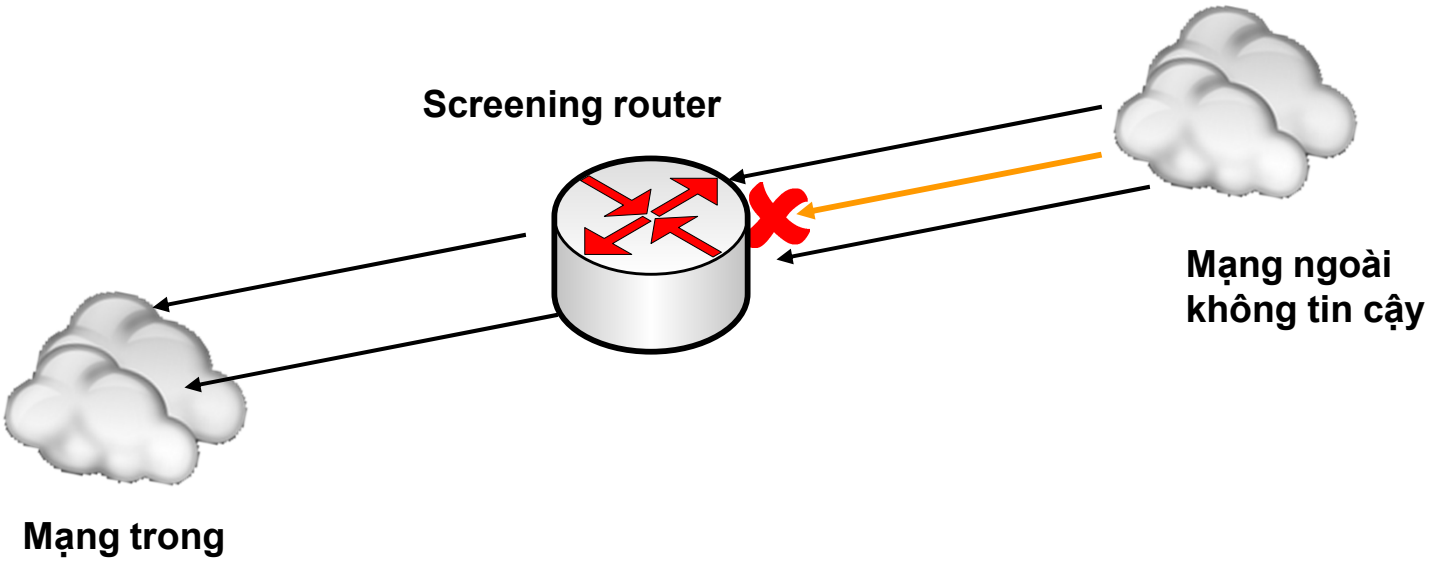
Chỉ cho phép những gói trả lại theo yêu cầu đặt ra
Khóa những đường truyền chưa đăng ký

Chu đề 7. Bảo mật mạng máy tính

✓ Các mô hình firewalls

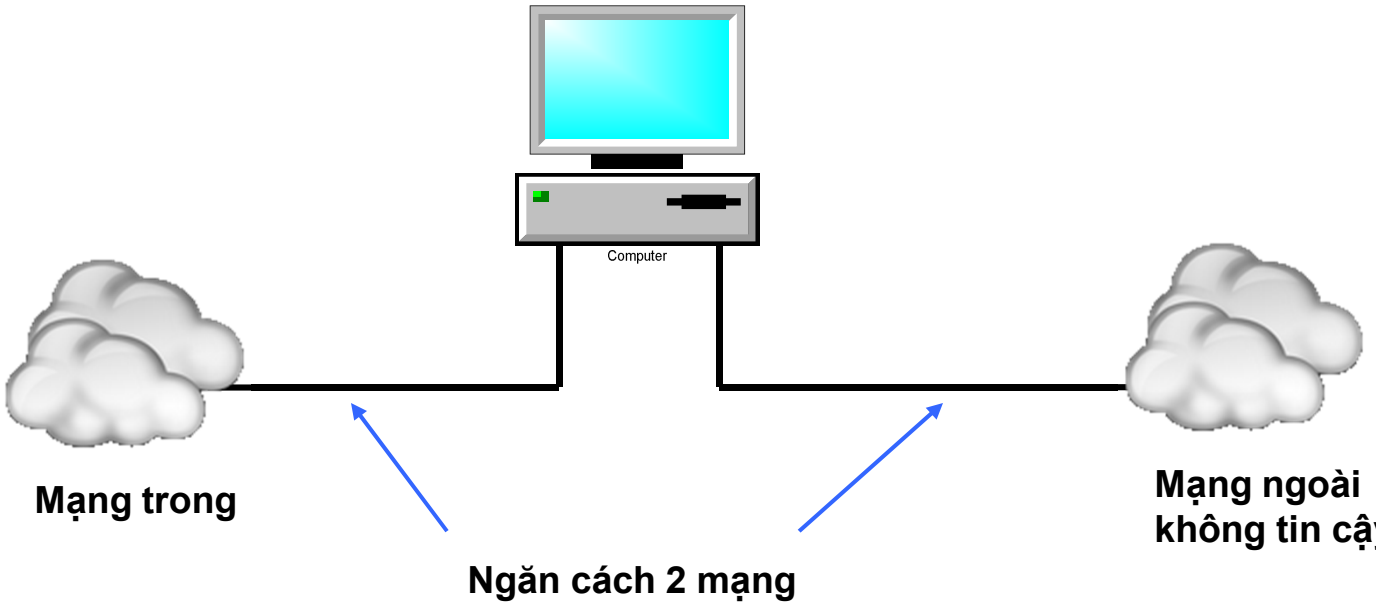
o Screening Routers

- Gồm một packet-filtering router đặt giữa mạng nội bộ và mạng Internet
- Chuyển tiếp truyền thông giữa 2 mạng và sử dụng các qui luật về lọc gói để cho phép hay từ chối truyền thông

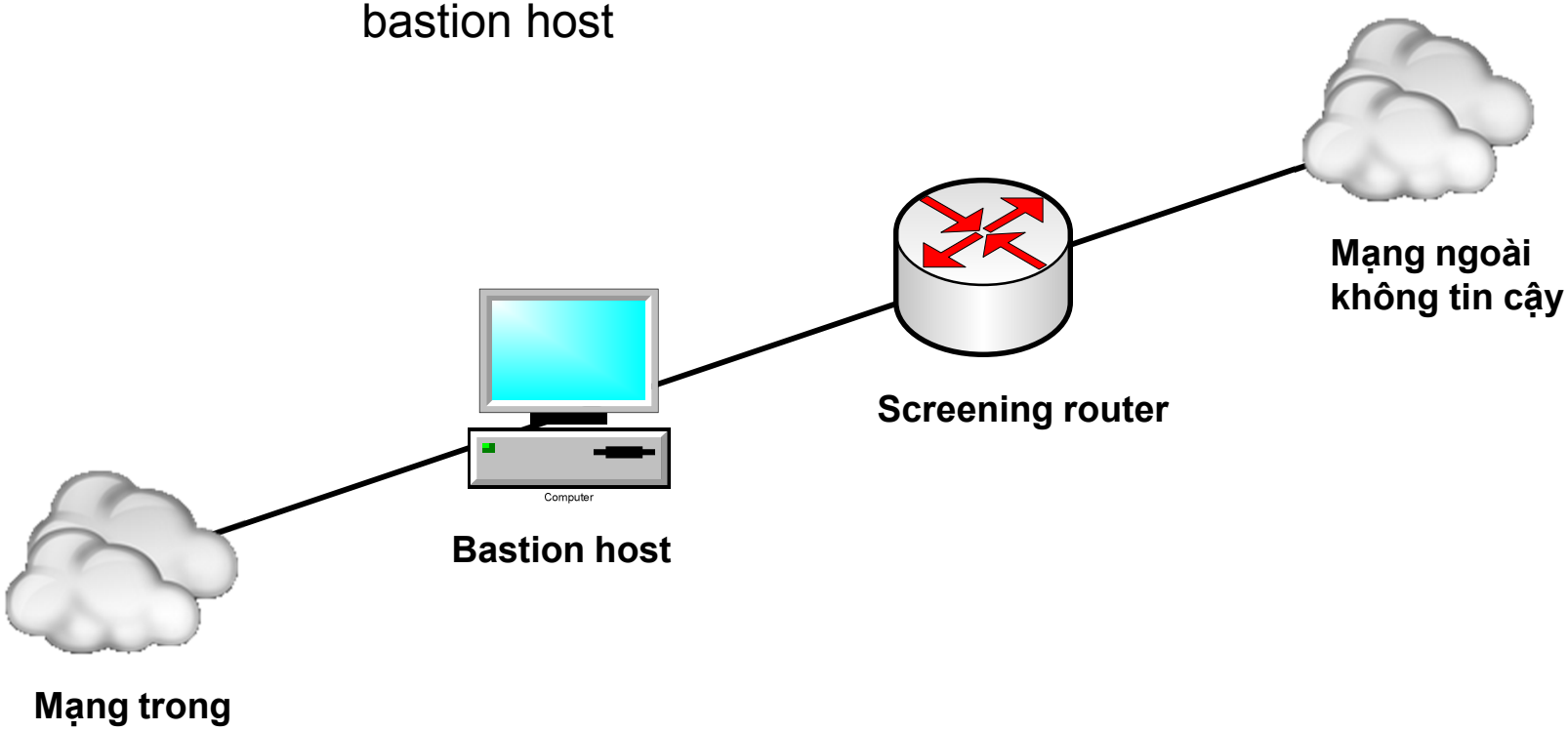


- **Dual-homed firewalls**
  - Các gói tin truyền đi được thông qua Proxy
  - Không cho phép truyền thông trực tiếp giữa 2 mạng giúp che giấu mạng bên trong với thế giới bên ngoài

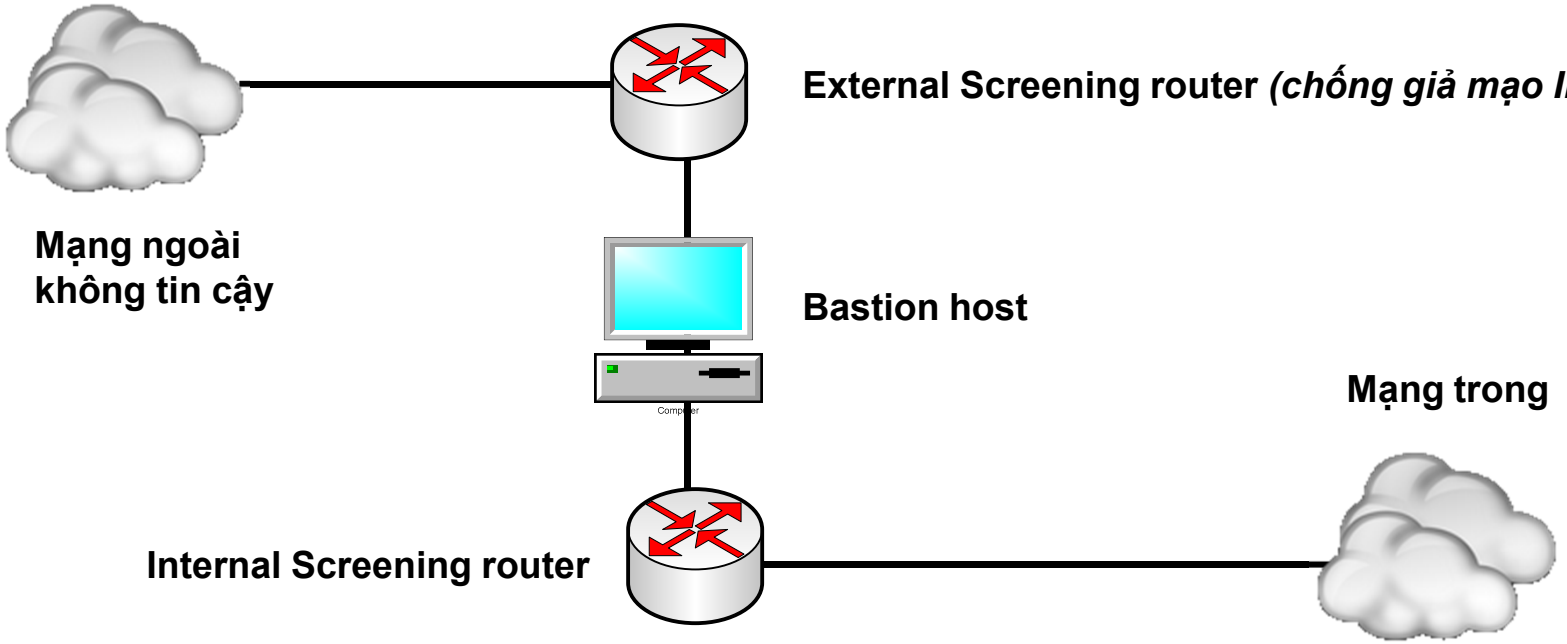
Dual-homed host



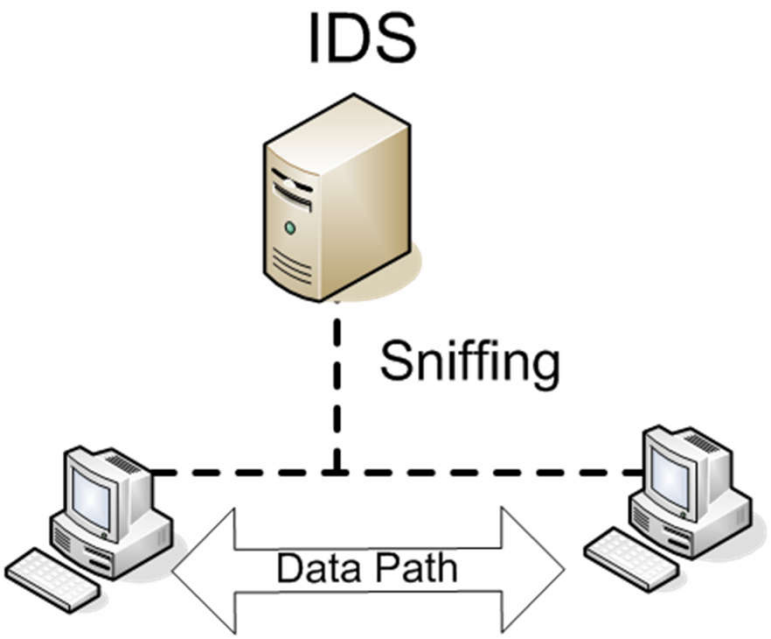
- **Screened host**
  - Bao gồm 1 packet-filtering router và 1 bastion host
  - Bastion host được cấu hình ở trong mạng nội bộ
  - Chỉ chấp nhận những truyền thông nội bộ xuất phát từ bastion host



- **Mô hình DMZ (Delimitarized Zone) hay Screened subnet**
  - Bao gồm 2 packet-filtering router và 1 bastion host
  - Có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật mạng (network) và mức ứng dụng (application)
  - Vùng DMZ đóng vai trò là một mạng nhỏ, cô lập, nằm giữa Internet và mạng trong



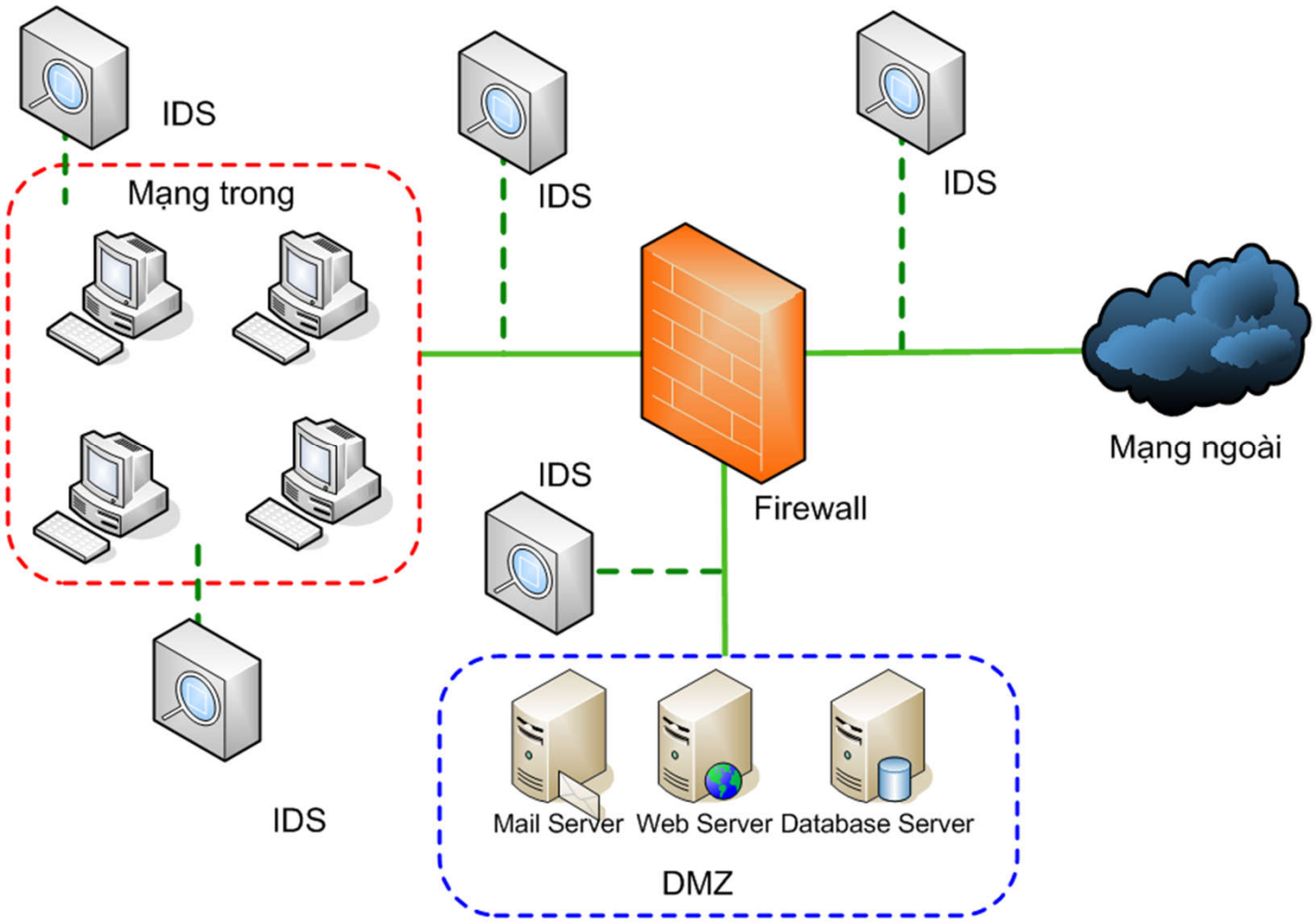
- **Instruction Detection System (IDS): Hệ thống phát hiện xâm nhập**
  - IDS phân tích các gói tin trong mạng (sniffer) để phát hiện các dấu hiệu khả nghi, thường đặt trong firewall



- **Chức năng**
  - Quản lý, phân tích hoạt động của người dùng và hệ thống
  - Kiểm tra cấu hình và tính toàn vẹn của hệ thống
  - Phân tích, phát hiện dấu hiệu các cuộc tấn công và lỗ hổng
  - Phân tích thống kê các dấu hiệu bất thường
  - Theo dõi các hành vi từ khi vào tới khi ra khỏi mạng
- **Hạn chế của IDS**
  - IDS chỉ là hệ thống phát hiện xâm nhập, nhưng chưa có khả năng chống lại.
  - Không giúp được cơ chế authentication và identification
  - Không giúp đỡ được sự yếu kém trong giao thức mạng
  - Không thể hỗ trợ tính toàn vẹn và tin cậy của dữ liệu
  - Không thể đáp ứng yêu cầu phân tích dữ liệu trong mạng tốc độ cao

- **Phân loại IDS**
  - Application based IDS
  - Host based IDS (HIDS)
  - Network based IDS (NIDS)
  - Hệ thống tích hợp (Intergrated IDS)
- **Nguyên lý hoạt động của IDS**
  - Phát hiện bất thường
    - Anomaly based analysis
    - Heuristic based analysis
    - Statistical
  - Phát hiện sử dụng sai mục đích
    - Pattern matching
    - Stateful pattern matching
    - Protocol decode-based analysis

- **Cấu hình một hệ thống mạng có IDS**



Chương trình mô phỏng quá trình lọc gói tin của firewall