CÁC CÔNG NGHỆ BẢO MẬT



CÔNG TY CỔ PHẦN CIS | Địa chỉ: Tòa nhà D4/D6, Khu Đô thị mới Cầu Giấy, phường Dịch Vọng, quận Cầu Giấy, Hà Nội. Điện thoại: (+84-4) 3513 3049/50, Fax: (+84-4) 3513 3051

NỘI DUNG

- Các công nghệ truyền thống
- Các công nghệ hiện nay
- Giải pháp

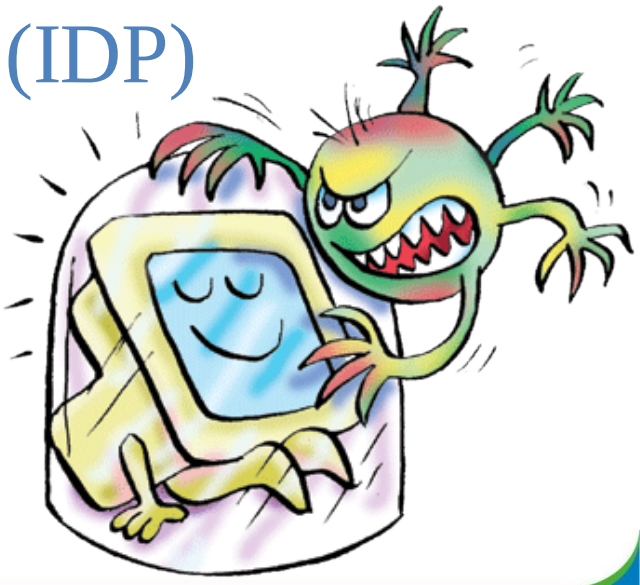
NỘI DUNG

Các công nghệ truyền thống

Công nghệ bảo mật truyền thống

Bao gồm hệ thống thiết bị, phần mềm:

- Phần mềm diệt virus (Antivirus - AV)
- Tường lửa (Firewall)
- Ngăn chặn phát hiện xâm nhập (IDP)



Phần mềm diệt virus AV

- Là phần mềm có tính năng phát hiện, loại bỏ các virus máy tính,
- Khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus trong tương lai.

Các kỹ thuật phát hiện, diệt virus

- So sánh với mẫu virus biết trước
- Nhận dạng hành vi đáng ngờ
- Kiểm soát liên tục
- Kết hợp mọi phương thức

Hệ thống phát hiện ngăn chăn xâm nhập IDP

- Phát hiện xâm nhập là quá trình giám sát, phân tích và ngăn chặn các sự kiện trong mạng
- Bao gồm:
  - IDS (Intrusion Detection System)
  - IPS (Intrusion Prevention System)
- Nguyên nhân:
  - Mã độc, sâu mạng, phần mềm gián điệp,
  - Kẻ tấn công đang kiếm quyền truy cập hợp pháp
  - Người sử dụng hợp lệ có các hành vi vượt qua các đặc quyền truy cập

Phân loại

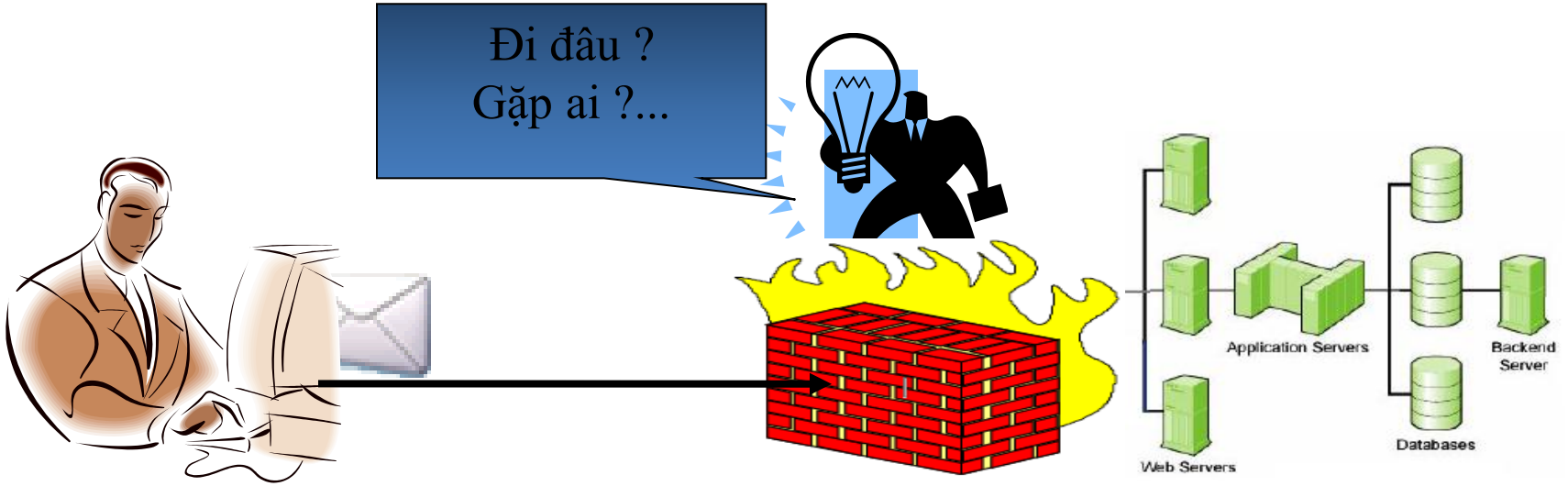
- IDS (Detection) được thiết kế với mục đích chủ yếu là phát hiện và cảnh báo các nguy cơ xâm nhập
- IPS (Prevention) ngoài khả năng phát hiện còn có thể tự hành động chống lại các nguy cơ theo các quy định được người quản trị thiết lập sẵn

Tường lửa (Firewall)

- Firewall là những thiết bị hoặc các hệ thống kiểm soát "traffic" giữa các mạng có mức độ an toàn khác nhau
- Firewall như một Barrier, trạm kiểm soát ở các điểm nối giữa các vùng

Cơ chế hoạt động

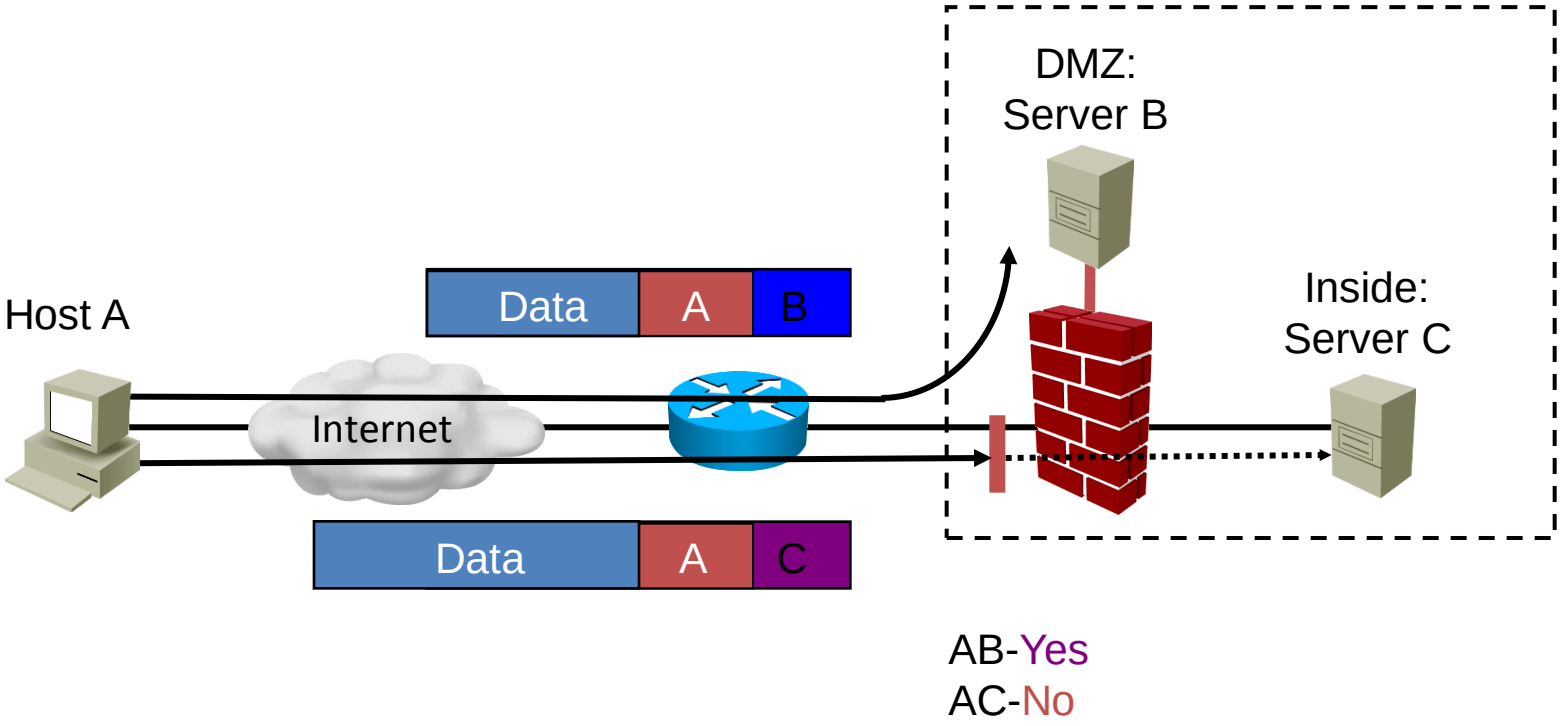
- Kiểm soát tất cả lưu thông và truy cập giữa các vùng cần bảo vệ
  - Những dịch vụ (port) nào bên trong được phép truy cập từ bên ngoài và ngược lại
  - Những node mạng (user, địa chỉ IP) nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong và ngược lại



Các công nghệ tường lửa

- Tường lửa lọc gói tin (Packet Filtering)
- Tường lửa kiểm soát trạng thái (Stateful packet filtering)
- Tường lửa mức ứng dụng Application,Proxy Server)

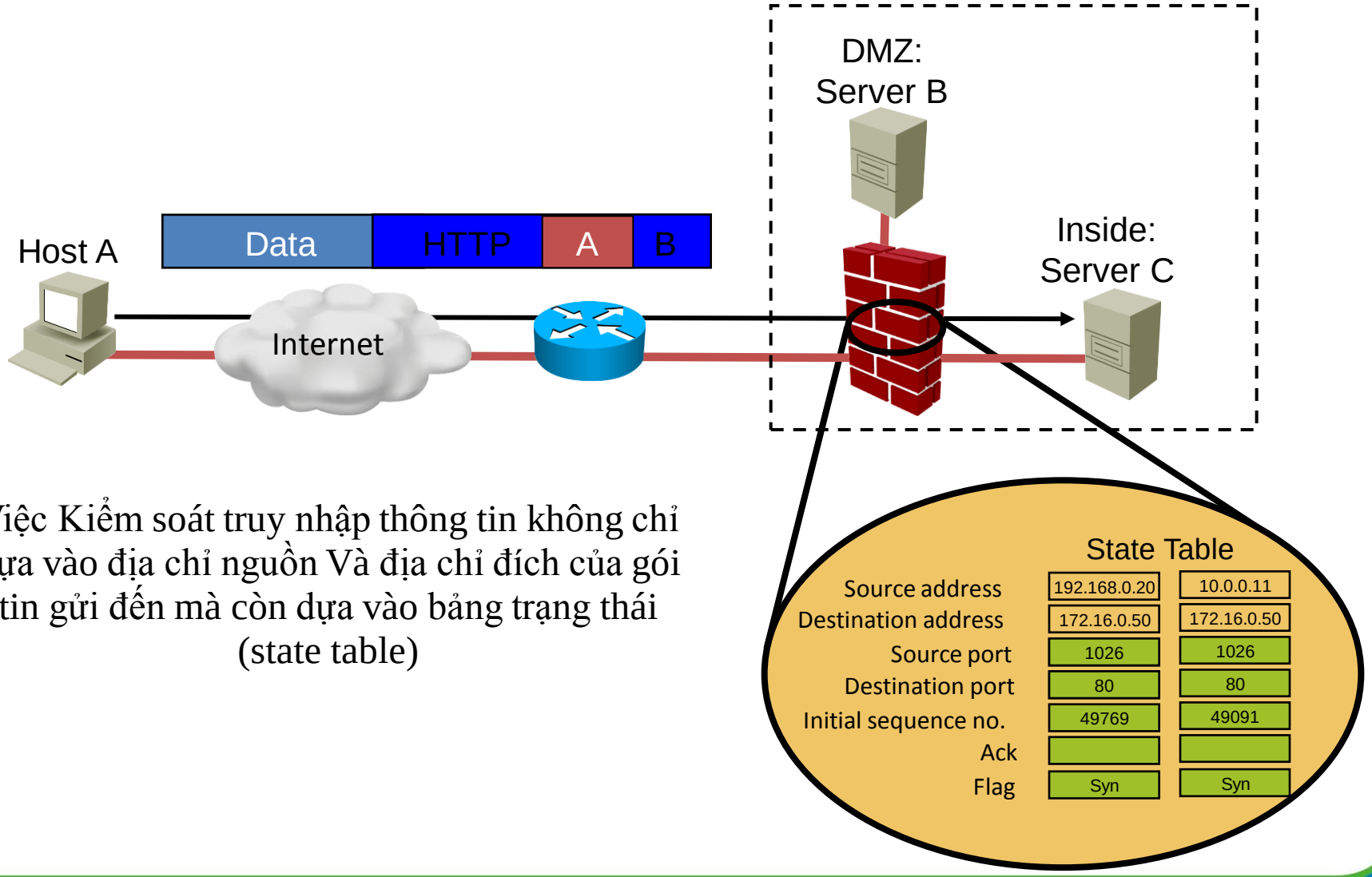
Packet Filtering



Việc Kiểm soát truy nhập thông tin dựa vào địa chỉ nguồn

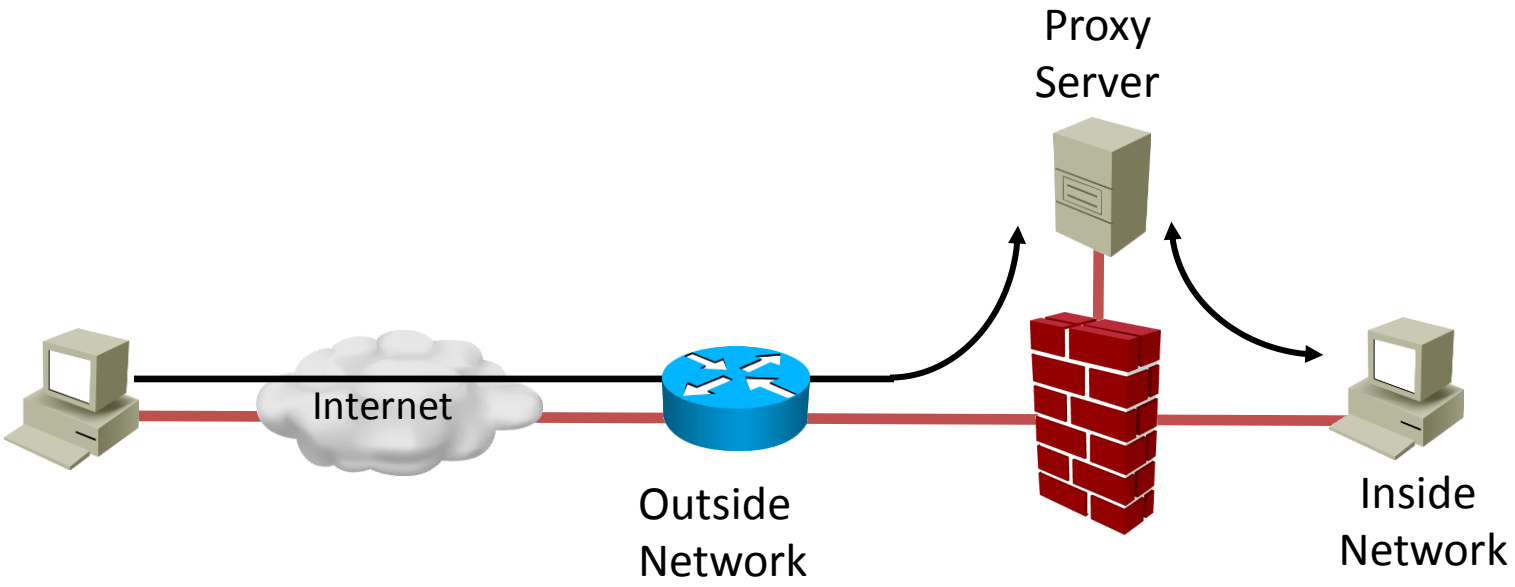
Và địa chỉ đích của gói tin gửi đến

Stateful Packet Filtering



Việc Kiểm soát truy nhập thông tin không chỉ dựa vào địa chỉ nguồn Và địa chỉ đích của gói tin gửi đến mà còn dựa vào bảng trạng thái (state table)

Proxy Server



Các kết nối từ được thông qua một máy chủ đại diện trung gian.

Firewall Rule

- Firewall Rule là các luật trên firewall, dựa vào đó Firewall đưa ra quyết định xử lý gói tin:

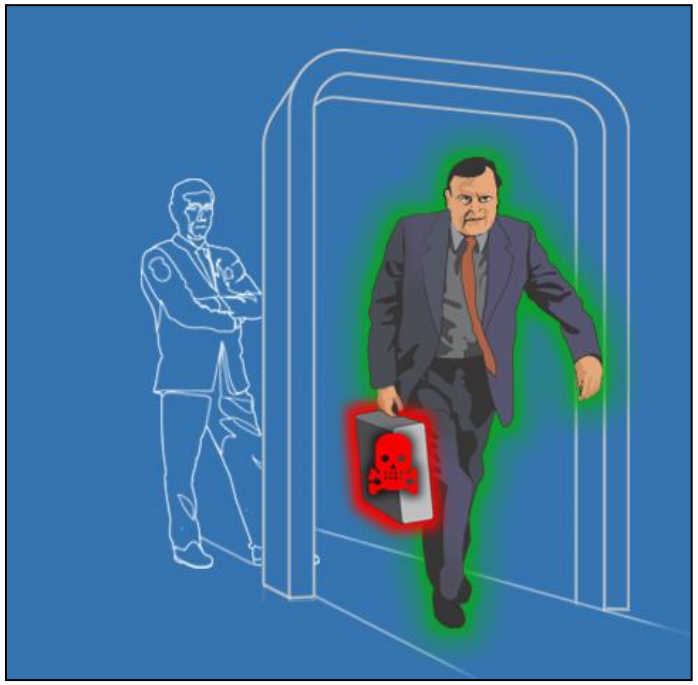
Source Address	Source Port	Destination Address	Destination Port	Action
192.168.0.1	any	any	80	allow
Any	Any	Any	Any	Drop

Lựa chọn Firewall

- Nên dùng các sản phẩm của các hãng "chuyên" về security
- Có khả năng hỗ trợ kỹ thuật tốt
- Có khả năng quản trị tập trung số lượng lớn firewall
- Ví dụ:
  - Firewall Cisco: PIX, ASA
  - Firewall Checkpoint, ISA, Astaro..

So sánh Firewall & Network IPS

- **Firewall:**
  - Như hệ thống xuất nhập cảnh
  - Kiểm soát Ai & Khi (Who & When) nào được phép đi qua
  - Kiểm soát dựa hộ chiếu
- **Network IPS:**
  - Như hệ thống hải quan
  - Kiểm soát cái gì và bằng cách nào (What & How) được phép đi qua
  - Kiểm soát dựa trên vật mang theo người



NỘI DUNG

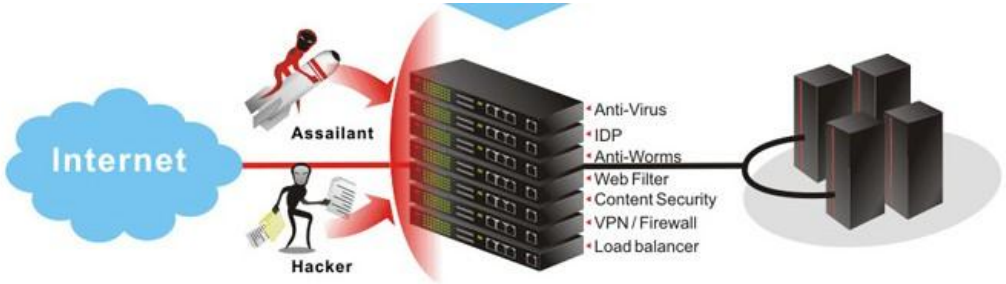
Các công nghệ hiện nay

Công nghệ bảo mật hiện nay

- Tường lửa đa chức năng (Unified Threat Management - UTM)
- Bảo mật điểm cuối (Endpoint)
- Chống thất thoát dữ liệu (Data Loss Prevention - DLP)
- Quản lý sự kiên an ninh (Security Information and Event Management - SIEM)
- Dò quét lỗ hổng bảo mật (Vulnerability Manager – VM)
- Quản lý truy cập mạng (Network Access Control – NAC)
- Bảo mật dữ liệu (Databases Security)
- Hệ thống bảo mật Web/Mail gateway
- …

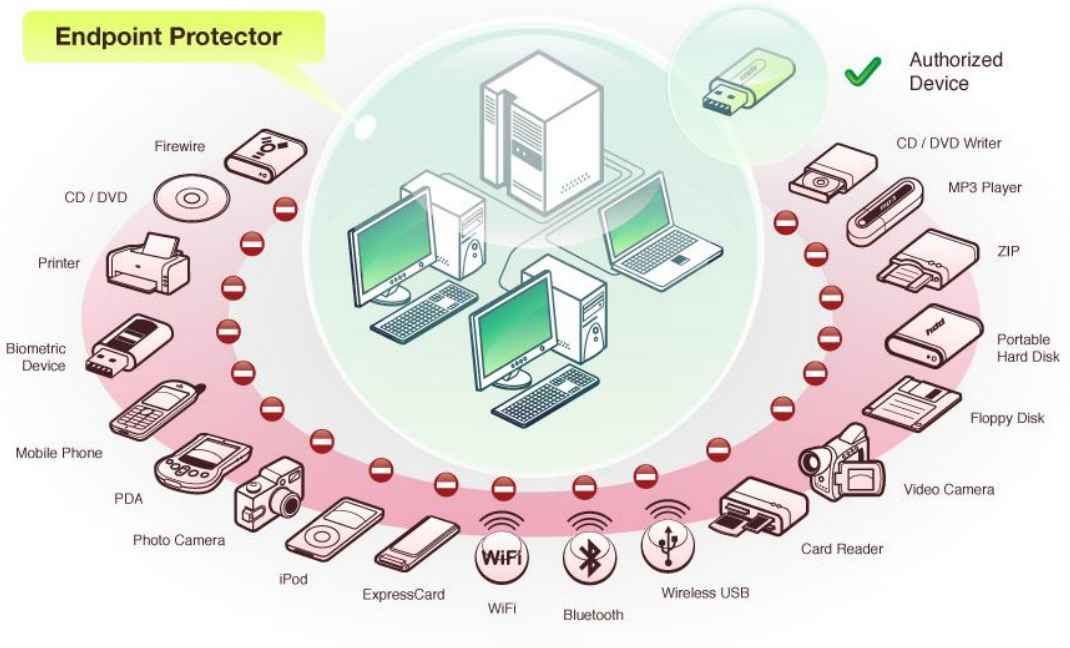
Tường lửa đa chức năng UTM

- Giải pháp tưởng lửa thế hệ mới, bảo vệ hệ thống mạng tổ chức trước các nguy cơ từ internet
- Tích hợp sẵn các tính năng
  - Firewall
  - IDP
  - AV, Filter
  - ..



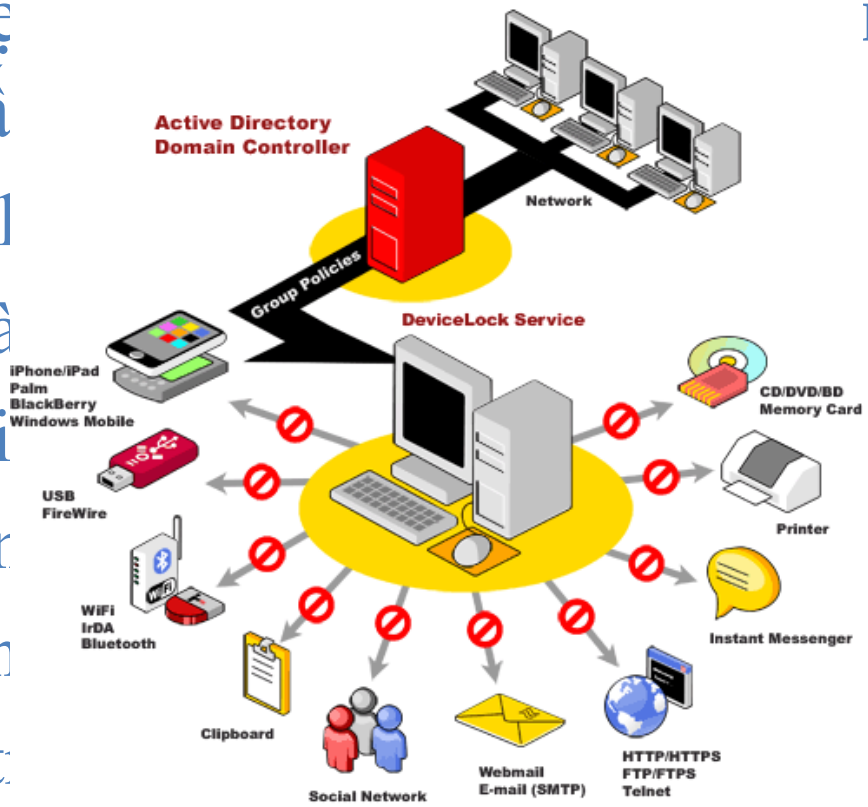
Bảo mật điểm cuối (Endpoint)

- Giải pháp bảo vệ tích hợp toàn diện, dễ dàng triển khai và quản trị
- Bao gồm
  - Hệ thống A
  - Lọc chăn th
  - Bảo vệ thiết
  - Hệ thống bả Smartphone
  - Hệ thống qu



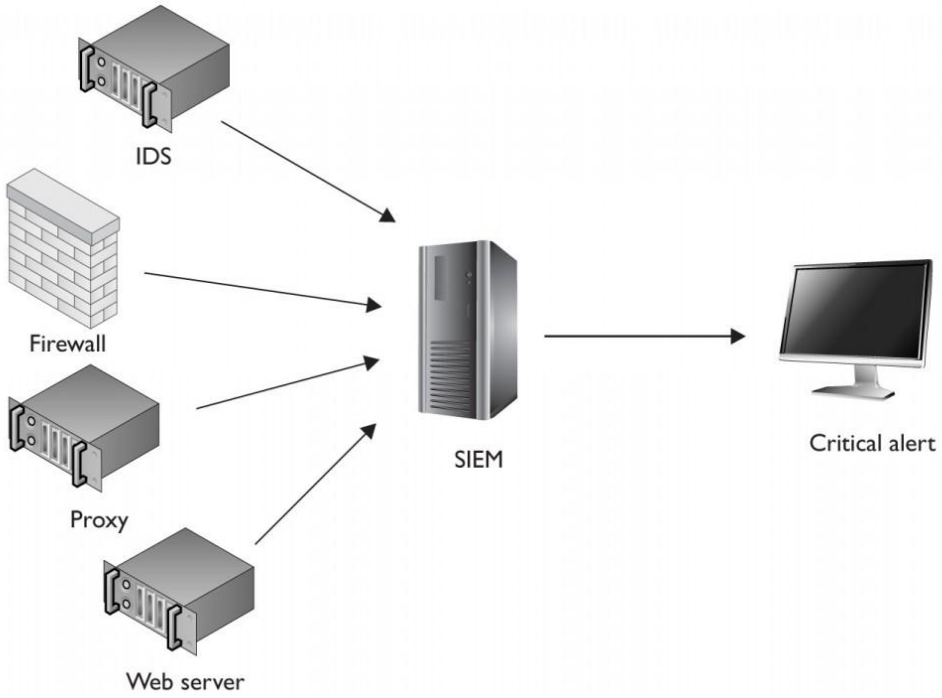
Chống thất thoát dữ liệu (DLP)

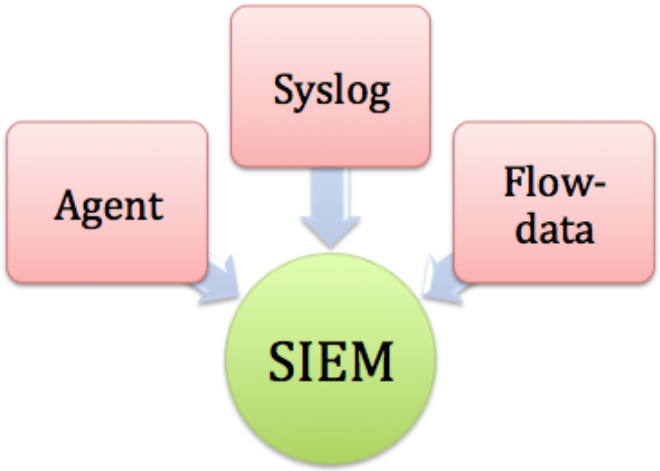
- Xác định dữ liệ ngăn chặn chống thấ
  - Tạo và phân l
  - Đưa ra các hà
  - Kiểm soát thi
  - Dễ dàng tạo r
  - Tạo và định n
  - Quản trị tập t
  - Kiểm tra vào



Quản lý sự kiện an ninh SIEM

ın ninh dễ dàng phát
:ơ, rủi ro trong hệ





– Lớp các thành phần tích hợp (Module Layer)

Dò quét lỗ hổng bảo mật (VM)

- Xác định các tài nguyên mạng, các lỗ hổng bảo mật đang tồn tại và đưa ra các hướng dẫn sửa chữa, khắc phục lỗ hổng nâng cao khả năng bảo mật của hệ thống
  - Dò quét, phát hiện các tài nguyên mạng
  - Dò quét, phát hiện các điểm yếu an ninh cho hệ thống mạng
  - Định danh mức độ rủi ro của hệ thống

NỘI DUNG

Giải pháp

Giải pháp

- Nâng cao vai trò của con người
- Lựa chọn chính xác vai trò, vị trí của công nghệ
- …

Các bước triển khai áp dụng

- Xác định mục tiêu, nhu cầu
- Xác định phạm vi
- Quy hoạch thiết kế hệ thống mạng
- Lập chính sách, xây dựng bộ luật
- Lựa chọn thiết bị bảo mật
- Triển khai và Theo dõi, cập nhật

Xác định mục tiêu

- An toàn vs Tốc độ (Security vs Performance)
- Kiểm soát truy cập đến mức nào:
  - Mức mạng (TCP IP)
  - Mức ứng dụng (Web)
  - Trên một vài Host hay toàn bộ mạng
- Quản lý tập trung hay phân tán

Xác định phạm vi

- Xác định mức độ an ninh, mức độ quan trọng:
  - Mức độ cao
  - Mức độ trung bình
  - Mức độ thấp
- Xác định mức độ an ninh hoặc khả năng bị tấn công, khả năng xuất hiện tấn công:
  - Máy chủ ứng dụng nghiệp vụ, CSDL
  - Máy quản trị
  - Máy chủ cung cấp dịch vụ công cộng
  - Máy trạm
  - Vùng thử nghiệm, lab

Lập Policy cho Firewall

- Traffic đi ra, đi vào mỗi vùng mạng cần được kiểm soát bởi firewall.
- Cần lưu ý: Chính sách trên firewall phải dựa trên chính sách của công ty hoặc được lãnh đạo phê duyệt

Cập nhật, giám sát

- Xây dựng quy trình bảo mật
- Lập lịch theo dõi giám sát hệ thống
- Có hệ thống nhật ký (log), báo cáo (Report)
- Dò quét, kiểm soát các lỗ hổng bảo mật
- Cập nhật định kỳ công nghệ, các bản vá lỗi

Thank You !