**Câu hỏi : Nêu nguyên tắc hoạt động của Firewall Sophos UTM và Domain Controller trong mô hình mạng đã thiết lập trong bài lab.**

* **Firewall Sophos UTM**

Sophos UTM (Unified Threat Management) là một giải pháp tường lửa doanh nghiệp với nhiều chức năng bảo mật. Trong bài lab, Sophos UTM được cấu hình để bảo vệ hệ thống mạng với hai vùng chính:

* **Mạng nội bộ (Internal)**: 10.0.0.0/8
* **Vùng DMZ (Demilitarized Zone)**: 172.16.0.0/16

Các nguyên tắc hoạt động của Sophos UTM trong bài lab:

* **Network Protection**:
  + Chặn các cuộc tấn công mạng từ bên ngoài và bên trong.
  + Tạo các quy tắc truy cập để kiểm soát lưu lượng mạng.
  + Hỗ trợ tính năng chống tấn công DoS, IPS (Intrusion Prevention System).
* **Web Protection**:
  + Kiểm soát quyền truy cập vào website theo danh sách quy tắc.
  + Chặn nội dung độc hại, lọc quảng cáo, kiểm soát tải xuống.
* **NAT (Network Address Translation)**:
  + Cấu hình NAT Outbound để cho phép thiết bị nội bộ truy cập Internet thông qua Firewall.
* **Kiểm soát truy cập Internet**:
  + Tạo quy tắc để cho phép Domain Controller có thể kết nối Internet.
  + Chặn truy cập từ các thiết bị trái phép vào hệ thống nội bộ.
* **Cấu hình và quản trị**:
  + Quản lý thông qua WebAdmin tại địa chỉ https://10.0.0.1:4444.
  + Firewall hoạt động như một Gateway giữa mạng nội bộ, vùng DMZ và Internet.
* **Domain Controller (DC)**

Domain Controller trong bài lab sử dụng Windows Server 2008 với IP 10.0.0.2/8. Nó có vai trò quản lý tập trung hệ thống mạng nội bộ.

Các nguyên tắc hoạt động của Domain Controller trong bài lab:

* **Xác thực người dùng (Authentication)**:
  + Sử dụng Active Directory để xác thực tài khoản đăng nhập trong mạng nội bộ.
  + Cho phép hoặc từ chối truy cập vào tài nguyên mạng theo Group Policy (GPO).
* **Dịch vụ DNS**:
  + Hoạt động như một máy chủ DNS nội bộ (10.0.0.2), hỗ trợ phân giải tên miền trong mạng.
  + Cấu hình Forwarder DNS đến 8.8.8.8 để phân giải tên miền Internet.
* **Quản lý tài khoản và nhóm người dùng**:
  + Cho phép tạo và quản lý tài khoản người dùng trong mạng nội bộ.
  + Áp dụng chính sách bảo mật thông qua GPO.
* **Tích hợp với Firewall Sophos UTM**:
  + Được Firewall cấp quyền truy cập Internet sau khi cấu hình quy tắc phù hợp.
  + Hỗ trợ kiểm soát truy cập mạng thông qua hệ thống xác thực.