### Nguyên tắc hoạt động của ****Firewall Sophos UTM**** và ****Domain Controller**** trong mô hình mạng đã thiết lập trong bài lab:

#### ****1. Firewall Sophos UTM****

Sophos UTM (Unified Threat Management) là một giải pháp tường lửa thế hệ mới (Next-Gen Firewall) có chức năng bảo vệ hệ thống mạng khỏi các mối đe dọa từ bên ngoài và kiểm soát lưu lượng truy cập nội bộ. Nguyên tắc hoạt động của Sophos UTM trong bài lab bao gồm:

* **Lọc gói tin (Packet Filtering):** Kiểm soát các gói tin ra/vào dựa trên các quy tắc tường lửa đã thiết lập.
* **NAT (Network Address Translation):** Chuyển đổi địa chỉ IP để kết nối mạng nội bộ với mạng bên ngoài (Internet).
* **VPN (Virtual Private Network):** Cho phép kết nối từ xa an toàn vào hệ thống mạng nội bộ.
* **Web Filtering:** Chặn hoặc cho phép truy cập các website dựa trên danh sách cấm hoặc chính sách truy cập.
* **IPS (Intrusion Prevention System):** Giám sát và phát hiện các cuộc tấn công vào hệ thống mạng.
* **Quản lý băng thông (Bandwidth Management):** Giới hạn tốc độ truy cập Internet cho từng người dùng hoặc dịch vụ.
* **Authentication (Xác thực người dùng):** Kiểm soát quyền truy cập dựa trên tài khoản người dùng.

#### ****2. Domain Controller****

Domain Controller (DC) là máy chủ quản lý miền (Domain) trong hệ thống Windows Server, đóng vai trò chính trong việc xác thực người dùng và quản lý tài nguyên mạng. Nguyên tắc hoạt động của Domain Controller trong bài lab:

* **Active Directory (AD):** Lưu trữ thông tin người dùng, nhóm, máy tính và chính sách bảo mật của tổ chức.
* **Xác thực người dùng:** Khi một máy tính hoặc người dùng đăng nhập vào mạng, DC kiểm tra thông tin xác thực (username, password) và cấp quyền truy cập.
* **Quản lý chính sách nhóm (Group Policy):** DC áp dụng các chính sách bảo mật như giới hạn quyền truy cập, cài đặt ứng dụng bắt buộc, chặn USB...
* **DNS Server:** DC thường tích hợp dịch vụ DNS để phân giải tên miền trong nội bộ mạng.
* **Single Sign-On (SSO):** Người dùng chỉ cần đăng nhập một lần để truy cập nhiều dịch vụ khác nhau trong mạng nội bộ.