**C. CÂU HỎI**

Sau quá trình thực hành, sinh viên trả lời câu hỏi sau:

Nêu nguyên tắc hoạt động của Firewall Sophos UTM và Domain Controller trong

mô hình mạng đã thiết lập trong bài lab.

=> **Nguyên tắc hoạt động của Firewall Sophos UTM:**

Trong mô hình mạng đã thiết lập, **Firewall Sophos UTM** đóng vai trò là **cổng an ninh bảo vệ mạng nội bộ**, với các nguyên tắc hoạt động chính như sau:

* **Kiểm soát lưu lượng mạng**: Sophos UTM kiểm tra, lọc và kiểm soát các gói tin ra vào giữa mạng nội bộ và mạng bên ngoài (Internet), đảm bảo chỉ những lưu lượng hợp lệ và được cho phép mới được truyền qua.
* **Chính sách tường lửa (Firewall Rules)**: Các chính sách được cấu hình để cho phép hoặc chặn truy cập dựa trên địa chỉ IP nguồn/đích, giao thức, cổng dịch vụ… đảm bảo an toàn cho hệ thống.
* **NAT (Network Address Translation)**: Thực hiện chuyển đổi địa chỉ IP nội bộ sang IP công cộng khi truy cập Internet, bảo vệ thông tin nội bộ và tiết kiệm tài nguyên IP.
* **Chống xâm nhập và quét cổng**: Sophos UTM có thể tích hợp tính năng chống xâm nhập (IPS/IDS) để phát hiện các hành vi tấn công mạng và cảnh báo/quản lý kịp thời.
* **VPN và truy cập từ xa**: Cho phép cấu hình VPN để người dùng truy cập an toàn vào mạng nội bộ từ bên ngoài.

**Nguyên tắc hoạt động của Domain Controller (DC):**

Trong mô hình, **Domain Controller** là máy chủ quản lý **dịch vụ Active Directory** và thực hiện các chức năng sau:

* **Xác thực người dùng**: Domain Controller xác thực tài khoản người dùng khi đăng nhập vào domain (tên người dùng, mật khẩu), đảm bảo chỉ người dùng hợp lệ mới được truy cập vào hệ thống.
* **Quản lý tập trung tài nguyên mạng**: Domain Controller quản lý các đối tượng như người dùng, máy tính, nhóm, chính sách GPO (Group Policy) và tài nguyên mạng một cách tập trung.
* **Cấp phát chính sách bảo mật**: Thông qua Group Policy, DC áp dụng các chính sách bảo mật cho người dùng và máy trạm như cấu hình mạng, hạn chế quyền truy cập, cập nhật hệ thống,…
* **Phân giải tên trong domain**: DC hoạt động như một DNS Server nội bộ, giúp phân giải tên miền nội bộ (ví dụ: client01.domain.local) thành địa chỉ IP.