Họ và tên : Trần Lệ Uyên

Lớp : 10CNPM2

MSSV : 1050080165

Bài tập lab 3 + lab 5

Lý thuyết lab 3 :

1. **Firewall Sophos UTM**

Firewall Sophos UTM (Unified Threat Management) là một giải pháp tường lửa bảo mật đa lớp, thực hiện các chức năng quan trọng như:

* **Kiểm soát luồng dữ liệu**: Lọc và kiểm soát truy cập dựa trên các chính sách định sẵn, kiểm tra nguồn và đích của gói tin.
* **Chống tấn công mạng**: Phát hiện và ngăn chặn các mối đe dọa như DDoS, xâm nhập trái phép (IPS - Intrusion Prevention System).
* **Quản lý VPN**: Hỗ trợ kết nối VPN (IPSec, SSL, L2TP) để bảo mật truy cập từ xa.
* **Lọc nội dung Web**: Áp dụng chính sách lọc web, ngăn chặn truy cập vào các trang web độc hại hoặc không phù hợp.
* **Quản lý băng thông**: Kiểm soát và phân bổ băng thông hợp lý theo từng nhóm người dùng hoặc ứng dụng.
* **Chính sách NAT và Routing**: Chuyển tiếp và ánh xạ cổng dịch vụ, đảm bảo kết nối nội bộ và internet ổn định..

1. **Domain Controller (DC) trong hệ thống mạng**

Domain Controller (DC) là một máy chủ quan trọng trong hệ thống Windows Server, đảm nhận các vai trò:

* **Xác thực người dùng**: Sử dụng Active Directory (AD) để xác thực danh tính người dùng trong mạng.
* **Quản lý tài khoản và quyền truy cập**: Phân quyền theo nhóm (GPO - Group Policy Objects) để kiểm soát tài nguyên trong hệ thống.
* **Tích hợp với Firewall Sophos UTM**: Có thể triển khai Single Sign-On (SSO) để đồng bộ hóa chính sách bảo mật giữa tường lửa và hệ thống xác thực người dùng.
* **Quản lý DNS và DHCP**: Cung cấp dịch vụ DNS nội bộ để định danh và phân giải tên miền, DHCP để cấp phát IP động.
* **Ghi log và giám sát**: Ghi nhận nhật ký đăng nhập, hoạt động của người dùng để hỗ trợ kiểm soát bảo mật.