Họ và Tên : Giang Thị Sông Hằng

Lớp :CNPM2

**1. Nguyên tắc hoạt động của Firewall Sophos UTM**

Firewall Sophos UTM (Unified Threat Management) là một giải pháp bảo mật mạng đa lớp, hoạt động theo các nguyên tắc sau:

* **Lọc gói tin (Packet Filtering):** Kiểm tra các gói tin ra/vào dựa trên các quy tắc bảo mật do quản trị viên thiết lập.
* **Tường lửa trạng thái (Stateful Firewall):** Theo dõi trạng thái kết nối của từng phiên làm việc, đảm bảo rằng chỉ các gói tin hợp lệ mới được phép truyền qua.
* **Kiểm soát truy cập (Access Control):** Xác định quyền truy cập vào các tài nguyên mạng dựa trên địa chỉ IP, giao thức, cổng kết nối, v.v.
* **NAT (Network Address Translation):** Chuyển đổi địa chỉ IP riêng (Private IP) sang địa chỉ công cộng (Public IP) để kết nối Internet.
* **VPN (Virtual Private Network):** Hỗ trợ kết nối từ xa an toàn thông qua VPN (SSL VPN, IPsec VPN).
* **Chống tấn công mạng (Intrusion Prevention System - IPS):** Giám sát và ngăn chặn các hành vi xâm nhập trái phép vào hệ thống.
* **Lọc nội dung (Web Filtering):** Kiểm soát truy cập web dựa trên danh mục, nội dung và chính sách bảo mật.
* **Chống virus và phần mềm độc hại:** Tích hợp hệ thống quét virus giúp bảo vệ hệ thống khỏi các mối đe dọa trực tuyến.

**2. Nguyên tắc hoạt động của Domain Controller (DC)**

Domain Controller là một máy chủ trong hệ thống Windows Server dùng để quản lý và xác thực người dùng trong mạng theo nguyên tắc:

* **Xác thực người dùng (Authentication):** Sử dụng giao thức **Kerberos** hoặc **NTLM** để kiểm tra danh tính người dùng khi đăng nhập vào hệ thống.
* **Quản lý tài khoản và chính sách (Account & Policy Management):** Lưu trữ thông tin người dùng, nhóm, quyền hạn trong Active Directory (AD).
* **Ủy quyền truy cập (Authorization):** Kiểm soát quyền truy cập vào tài nguyên mạng như tệp tin, thư mục, máy in, ứng dụng, v.v.
* **Đồng bộ hóa và sao lưu dữ liệu (Replication & Backup):** Đồng bộ dữ liệu giữa nhiều Domain Controller trong hệ thống để đảm bảo tính liên tục của dịch vụ.
* **Cấp phát địa chỉ và tài nguyên mạng:** Kết hợp với **DHCP, DNS** để quản lý hệ thống mạng nội bộ một cách hiệu quả.