**Đinh Minh Tài**

**1050080115**

**Bài làm**

**Lab 4: Sophos UTM Firewall Rules**

**1. Mục tiêu của bài Lab**

* Hiểu cách tạo và quản lý các quy tắc tường lửa (Firewall Rules) trong Sophos UTM.
* Cấu hình chính sách bảo mật để kiểm soát lưu lượng mạng.
* Thực hành chặn và cho phép truy cập dựa trên địa chỉ IP, dịch vụ và giao thức.

**2. Yêu cầu chuẩn bị**

* Một máy ảo hoặc thiết bị cài đặt Sophos UTM.
* Truy cập vào giao diện quản trị WebAdmin.
* Các tài nguyên mạng để kiểm tra hoạt động của tường lửa.

**3. Hướng dẫn thực hiện**

**Bước 1: Đăng nhập vào Sophos UTM WebAdmin**

1. Mở trình duyệt và truy cập: https://<địa chỉ\_IP>:4444.
2. Đăng nhập bằng tài khoản quản trị viên.

**Bước 2: Tạo quy tắc Firewall mới**

1. Điều hướng đến **Network Protection > Firewall**.
2. Chọn **New Rule** để tạo một quy tắc mới.
3. Cấu hình quy tắc như sau:
   * **Source (Nguồn)**: Chọn địa chỉ IP hoặc nhóm mạng cần áp dụng.
   * **Service (Dịch vụ)**: Chọn giao thức như HTTP, HTTPS, FTP, v.v.
   * **Destination (Đích)**: Chọn địa chỉ hoặc phạm vi cần kiểm soát.
   * **Action (Hành động)**: Chọn "Allow" để cho phép hoặc "Deny" để chặn.
4. Nhấn **Save** để lưu quy tắc.
5. Kéo thả quy tắc lên đầu danh sách để đảm bảo áp dụng đúng thứ tự.
6. Nhấn **Apply** để kích hoạt quy tắc.

**Bước 3: Kiểm tra quy tắc Firewall**

1. Sử dụng lệnh ping hoặc trình duyệt web để kiểm tra truy cập đến các địa chỉ bị chặn hoặc cho phép.
2. Mở **Log & Reports > Firewall Log** để kiểm tra các yêu cầu bị chặn hoặc cho phép.

**4. Bài tập thực hành**

1. Tạo một quy tắc **chặn toàn bộ truy cập internet** từ một địa chỉ IP cụ thể.
2. Tạo quy tắc **cho phép truy cập HTTP & HTTPS** từ mạng nội bộ ra internet.
3. Kiểm tra lại log tường lửa để xác minh các quy tắc hoạt động đúng.

**5. Kết luận**

* Sophos UTM cung cấp một giao diện trực quan để tạo và quản lý quy tắc tường lửa.
* Việc kiểm soát lưu lượng mạng giúp tăng cường bảo mật và tối ưu hóa hiệu suất mạng.
* Kiểm tra log firewall giúp xác minh các quy tắc đang hoạt động như mong đợi.