BÁO CÁO SỰ CỐ AN NINH MẠNG

# Phần 1: Tóm tắt sự cố

Trong quá trình phân tích log tcpdump, phát hiện rằng máy trạm (IP 192.51.100.15) đã gửi nhiều truy vấn DNS (giao thức UDP, cổng 53) đến máy chủ DNS (203.0.113.2) để phân giải tên miền yummyrecipesforme.com. Tuy nhiên, thay vì phản hồi thông tin phân giải, máy chủ DNS trả về thông báo lỗi ICMP 'udp port 53 unreachable'. Điều này cho thấy cổng 53 trên máy chủ DNS không sẵn sàng phục vụ hoặc bị chặn, dẫn đến việc không thể phân giải tên miền.

# Phần 2: Phân tích chi tiết

- Thời điểm sự cố được báo cáo: Người dùng bắt đầu báo lỗi khi truy cập website và nhận thông báo 'destination port unreachable'.  
- Triệu chứng: Không thể truy cập website www.yummyrecipesforme.com.  
- Quan sát từ log tcpdump:  
 + Nhiều truy vấn DNS được gửi đi bằng UDP.  
 + Máy chủ DNS liên tục trả về lỗi ICMP 'udp port 53 unreachable'.  
- Giải thích: Lỗi xuất hiện vì dịch vụ DNS không hoạt động hoặc có tường lửa/ngăn chặn chặn UDP port 53.

# Phần 3: Tình trạng hiện tại

Người dùng vẫn không thể truy cập website do không phân giải được địa chỉ IP của tên miền.

# Phần 4: Bước tiếp theo / Đề xuất giải pháp

1. Kiểm tra trạng thái hoạt động của dịch vụ DNS trên máy chủ 203.0.113.2.  
2. Xác minh cấu hình firewall có đang chặn UDP port 53 không.  
3. Đảm bảo dịch vụ bind/named đang chạy và lắng nghe trên cổng 53.  
4. Cung cấp DNS dự phòng cho người dùng (ví dụ Google DNS 8.8.8.8) để tạm thời đảm bảo truy cập.

# Phần 5: Nguyên nhân gốc rễ nghi ngờ

Sự cố nhiều khả năng xuất phát từ việc dịch vụ DNS trên máy chủ 203.0.113.2 bị tắt hoặc chặn UDP port 53, dẫn đến không thể xử lý các truy vấn phân giải tên miền.